Policy

**INTERNET AND ELECTRONIC COMMUNICATION**

*Code*  *Issued*

Hampton District One Schools makes a variety of communication and information technologies available to authorized users. The board supports the use of these technologies to improve teaching and learning through interpersonal communication, access to information, research, training and collaboration, and dissemination of successful educational practices, methods, and materials. When properly used, these technologies promote the District’s goals and objectives. Illegal, unethical, or inappropriate use can have significant negative consequences for the District, its students, and its employees. This policy is intended to minimize the likelihood of such harm by setting standards which protect the District, its users, its data, and its systems.

Generally, employees are expected to protect the health, safety, and emotional well-being of students and to preserve the integrity of the learning environment. Employees should preview and assess the appropriateness of any content accessed using district technology devices, accessed through the district network, and/or shared with students. Online or electronic conduct that distracts or disrupts the learning environment; adversely affects the reputation or image of the school district, the staff, or the board; or other conduct in violation of this or related district policies may form the basis for disciplinary action, up to and including termination.

**Technology Protection Measures**

In compliance with the Children’s Internet Protection Act (CIPA), 47 USC §254(h), Hampton One uses technological devices designed to filter and block the use of any technology devices from accessing materials that would be harmful to minors including, but not limited to retrieving or transmitting anything that is obscene, child pornography or “harmful to minors” as defined by the Children’s Internet Protection Act (CIPA).

Adult users of a district computer with Internet access may request, through the district work order system, that the “technology protection measures” be temporarily disabled for a specific valid site for educational research purposes or other lawful purposes not otherwise inconsistent with this acceptable use policy.

**Scope**

This policy governs all technology users (students and adults) and applies at all times and in all locations whether on or off District Property. Further this policy governs the use of all electronic systems owned, provided, or subscribed to by the District, including computers and computer-like devices, mobile devices, voice and data communication systems, networks, software, services, and personally owned devices connected to the district network.

District employees, contractors, and vendors will sign this policy prior to account access. Employees will take responsibility for their own use of district technology devices and the district network to ensure compliance with board policy.

Students are bound by an opt-out mechanism: parents not wishing for their child to be allowed access to computer networks, Internet, or other communication services must so indicate in writing to the school’s Principal. Each school will include an age appropriate version of this policy in the student handbook.

Under certain circumstances, the use of personally-owned computing and communication devices may be allowed on District property. These non-District-owned devices access District services, networks, data, and services, and as such are bound by this policy. Such devices are the sole responsibility of the owners. Owners of these devices are solely responsible for the configuration, content, upkeep, and safety of their devices. The District will not assist with configuration, will not troubleshoot issues, and assumes no responsibility for function or safety.

Guest user access can be arranged for lecturers, program presenters, or other event-based needs by arrangement with Technology Services. The Technology Services Help Desk can provide credentials for such users who are bound by this policy. Guest access is limited in terms of Internet and file access.

**No Expectation of Privacy**

District administration will continuously monitor all uses of district technology devices and the district network. The superintendent and/or his/her designee are authorized to access, inspect, monitor, and/or store any computer files, emails, internet usage logs, or any other electronic data at any time and for any purpose without staff consent or authorization. Technology users have no expectation of privacy in their use of district technology devices or the district network. Information considered to be confidential or personal should not be transmitted through district systems except via means designed or approved for that purpose by the Technology Department. The district assumes no responsibility for lost or stolen personal information sent or received via or stored on District systems.

Technology users are expected to cooperate fully with any investigation concerning or relating to the use of district technology. The district will cooperate fully with local, state, or federal officials in any investigation concerning or related to any illegal activities conducted with district technology devices or through the district network.

**Public Records**

Electronic communications sent and received by district employees may be considered public records subject to public disclosure or inspection under the South Carolina Freedom of Information Act. Employees should ensure that all electronic communications are professional in tone and content and are made for the express purpose of furthering the educational goals of the district.

**Unauthorized and Unacceptable Uses**

Because of the rapid evolution of technology, every possible use of district technology devices cannot be addressed in board policy. If a technology user has a question regarding the appropriateness of a given use of technology, he/she should consult his/her direct supervisor or building principal for guidance.

All technology users are prohibited from the use of district resources to view, access, create, download, transmit, display, store, or forward any material that violates any school or district policy or rule, or violates any local, state, or federal law or regulation.

Prohibited material includes, but is not limited to:

* Pornographic, obscene, or other sexually oriented materials
* Material promoting violence or advocating destruction of property including, but not limited to, access to information concerning the manufacturing or purchasing of destructive devices or weapons
* Material which could reasonably be construed as harassing, bullying, or discriminatory
* Material used to further any commercial business, political party, or other organization not specifically endorsed or supported by the District
* Material protected by copyright or trade secret; plagiarism
* Material which is potentially disruptive of the District’s instructional and business processes, including viruses, malware, spam, and tools or software intended to bypass, interrupt, or disable District security, filtering, or data-protection measures

Prohibited activities include but are not limited to:

* Attempts to access data or services to which the user has no District-defined need or permission
* Attempts to bypass, interrupt, or disable District security, filtering, or data-protection measures; hacking
* Use of a network access account other than that issued to you, or allowing (by any means) use of your account by anyone else; impersonation, misrepresentation of identity
* Operating or using a non-District network on District property, such as rogue Wi-Fi, MiFi, mobile hot-spots, or other network technology
* Attaching any personally-owned device to the District’s wired network without the explicit permission of the Technology Department
* Student use of a staff-owned personal device
* Transmission or transportation of confidential or privileged data (such as student information or records, personally-identifying information, District financial data, or personnel data) without authorization, or via a means which make the data subject to loss
* Use of District resources for commercial purposes or personal monetary gain; conducting personal financial activities; providing goods or services or purchasing goods or services for personal use.
* Use of District resources to send unsolicited messages unrelated to District business, chain messages, spam, or bulk messages
* Installing software not approved or allowed by Technology Services, particularly any which interfere with the intended operation of the system
* Alteration of or damage to District resources
* Threats against persons or property or activities that harass, threaten, demean, or promote violence or hatred against another person or group of persons with regard to race, religion, sex (including pregnancy, childbirth, or any related medical condition), color, disability, age (40 or older), genetic information, national origin, or marital status
* Using inappropriate or profane language likely to be offensive to others
* Violating third-party copyright or license agreements or engaging in activities that otherwise constitute unauthorized use of and/or copying of materials

**Use of Electronic Communication Tools**

Electronic communication tools, including, but not limited to, student email accounts, learning management platforms, or District-approved social networking sites, may be provided by the District. Technology Users must abide by the guidelines established in this document while using all electronic communication tools.

**Students** are only permitted to access email accounts provided by the district. Accessing personal email accounts is not allowed. Student Internet access will be under the direction and guidance of a District staff member. In addition, all students in grades K-12 will receive instruction on Internet safety and cyberbullying each school year.

**Violations and Consequences**

Users who observe or become aware of violations of this policy are required to report them to a teacher, administrator, supervisor, or Technology Director immediately. Failure to do so is itself a violation of this policy.

Upon discovery of violations or threats to the proper function of District systems, the Technology Department will act to protect data and systems. User accounts and or computers may be suspended or isolated to mitigate threats. Account suspension will be communicated to the Principal (in the case of student involvement), to the Supervisor and Human Resources (in the case of employee involvement), or to the sponsoring department (in the case of a vendor or contractor).

Violation of this policy by District employees may result in disciplinary action up to and including termination. Disciplinary action is the responsibility of Human Resources. Typically, a first violation may be met with a suspension of access privileges and a formal reprimand. Second or subsequent violations may be dealt with more severely.

Violation of this policy by students is within the scope of the Student Code of Conduct. The school’s disciplinary process will be followed.

Violation of this policy by contractors, vendors, or other authorized users who are not District employees may result in revocation of access privilege or other consequence as defined by the District.

**Limitation of Liability**

Hampton District One will not be responsible for damage or harm to persons, files, data, or hardware, including personally-owned devices.

The District employs security and filtering mechanisms and attempts to ensure their proper functioning, but can make no guarantee regarding their effectiveness.

**Personal Responsibility**

By accepting your user identification and password and related information, and / or by accessing Hampton District One technology resources, you agree to adhere to this Policy. You also agree to report any network or Internet misuse or abuse.

I have read and understand the Acceptable Use Policy for Technology.

Print Name Signature Date

Cf. IJNDB

Adopted ^

Legal references:

A. Federal Law:

1. Children’s Internet Protection Act (CIPA), 47 U.S.C.A. Section 254(h).
2. Digital Millennium Copyright Act (DMCA), 17 U.S.C.A. Section 512.
3. S.C. Code, 1976, as amended:
4. Section 10-1-205 - Computers in public libraries; regulation of Internet access.
5. Section 16-15-305 - Disseminating, procuring, or promoting obscenity unlawful; definitions; penalties; obscene material designated contraband.
6. Section 30-4-10, *et seq*. - Freedom of Information Act.