Mandatory Orientation/Acknowledgement. To educate students on proper Computer, Network, and Internet use and conduct, a mandatory orientation session is required by the end of the first six weeks each school year. Employees will receive a copy of the regulations and sign an acknowledgement form indicating that they have read and understand the regulations.

Availability of Access

Acceptable Use. Information technology resource access will be used to improve learning and teaching consistent with the educational goals of Dare County Schools. The District requires legal, ethical, and appropriate use of the information technology resources.

Privilege. Access to the Dare County Schools information technology resources is a privilege, not a right. Any users of theses resources, including staff and students, must comply with the following requirements. Any student's failure to comply may lead to serious disciplinary action. Any employee's failure to comply may lead to serious disciplinary action up to and including dismissal.

Access to Information Technology Resources. Information technology resources are provided to all Dare County Schools teachers and staff. Students may be allowed to use the local network with campus permission, but may only use the Internet and school-based email communication with parent permission. Student's Internet access will be under the direction and guidance of a Dare County Schools teacher or staff member. Access to the District's electronic communications system, including the Internet, shall be made to students and employees primarily for instructional and administrative purposes in accordance with this policy and regulations.

Subject to Monitoring. All Dare County Schools information technology resource usage shall not be considered confidential and is subject to monitoring by designated staff at any time to ensure appropriate use.

User Responsibilities. Information technology resource users, like traditional library users, are responsible for their actions.

1. Users with accounts will be required to maintain password confidentiality by not sharing the password with others. Users will also be required to logout of the network prior to leaving the computer.
2. Users are expected to use appropriate language: Swearing, vulgarity, ethnic or racial slurs, and any other inflammatory languages are prohibited.
3. Revealing such personal information as addresses or phone numbers of users to others is prohibited.
4. System users are asked to purge electronic mail or outdated files on a regular basis.
5. System users are responsible for making sure they do not violate any copyright laws.
6. Users are to notify the appropriate supervisor or district designee if they should encounter any material or electronic communication that is inappropriate.
7. System users may not use another person's system account.
8. System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.
9. A user who gains access to inappropriate material is expected to discontinue the access as quickly as possible. Students should report the incident to the supervising teacher; all other users should report the incident to the Technology Department.
10. A student who knowingly brings prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Board-approved Student Code of Conduct.
11. An employee who knowingly brings prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies.

12. Users who bring personal equipment into the school must coordinate with the technology staff prior to connecting it to the network. Dare County Schools will not be liable for any damage to and will not provide technical services to repair/fix personal equipment.
13. Students who are issued district-owned and maintained laptops must follow the guidelines in the district's Laptop Handbook for Students and Parents.
14. Those who use district-owned and maintained technologies to access the Internet at home are responsible for both the cost and configuration of such use.

Student Responsibilities. Students of Dare County Schools are bound by all portions of the Information Technology Resources Use Policy and Regulations.

Campus Level Responsibilities. The Principal or designee will:

1. Be responsible for disseminating and enforcing the Information Technology Resource Use Regulation for the District's system at the campus level.
2. Ensure that employees supervising students who use the District's systems provide information emphasizing the appropriate and ethical use of this resource.

Inappropriate Use Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of any components that are connected to the Information Technology Resources. The following actions are considered inappropriate uses and are prohibited:

Violations of Law. Transmission of any material in violation of any US or state law is prohibited. This includes, but is not limited to: copyrighted material; threatening, harassing, or obscene material; material protected by trade secret; or confidential information, or public records. Any attempt to break the law through the use of a Dare County Schools Information Technology Resources account may result in litigation against the offender by the proper authorities. If such an event should occur, Dare County Schools will fully comply with the authorities to provide any information necessary for the litigation process.

Modification of Computer. Modifying or changing computer settings and/or internal or external configurations without appropriate permission is prohibited.

Commercial Use. Use for the purpose of product advertisement, commercial, income-generating or "for-profit" activities is prohibited.

Vandalism/Mischief. Any malicious attempt to harm or destroy District equipment or materials, data of another user of the District's system, or any of the agencies or other networks to which the District has access is prohibited. Deliberate attempts to degrade or disrupt system performance may be viewed as violations of district policy and, possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges, possible prosecution, and will require restitution for costs associated with system restoration, hardware, or software costs.

Personal Websites and Social Networking Sites. The superintendent may use any means legally available and appropriate to request the removal of personal websites that substantially disrupt the school environment or that utilize school system or individual school names, logos or trademarks without permission.

1. Students
   Though school personnel generally do not monitor students' Internet activity conducted on non-school system computers during non-school hours, when a student's on-line behavior has a direct and substantial effect on school safety or maintaining order and discipline in the schools, the student may be disciplined in accordance with board policy (see the student behavior policies in the 4300 series).

2. Employees

   Employees are to maintain an appropriate professional relationship with students at all times. If an employee creates and/or posts inappropriate content on a website or profile and allows students access to the site, or if not, said content otherwise has a negative impact on the employee's ability to perform his or her job as it relates to working with students, the employee may be subject to appropriate discipline. This section applies to all employees, volunteers and student teachers working in the school system.

   For the purposes of this regulation, "social media" refers to the various online technology tools that enable people to communicate easily over the Internet to share information and resources. It includes, but is not limited to: personal websites, blogs, wikis, social networking sites, online forums, virtual worlds, video-sharing websites, and any other Internet-based applications which allow the exchange of user-generated content. For purposes of this regulation, it also includes any form of instant or direct messaging available through such applications. Examples of social media include Web 2.0 tools, Facebook, Twitter, LinkedIn, Flickr, YouTube, Instagram, Google+, and social media components of learning management systems such as Moodle or Edmodo. "Personal social media" means any social media networks, tools, or activities that are not school-controlled.

   As role models for the school system's students, employees are responsible for their public conduct even when they are not performing their job duties as employees of the school system. Employees will be held to the same professional standards in their public use of social media and other electronic communications as they are for any other public conduct.

   Employees are responsible for the content on their social media sites. Employees who use social media for personal purposes must be aware that the content they post may be viewed by anyone, including students, parents and community members. Employees shall observe the following principles when communicating through social media:

   1. Employees shall not post confidential information about students, employees or school system business.
   2. Employees shall be professional in all Internet postings related to or referencing the school system, students or their parents, and other employees.
   3. Employees shall not use profane, pornographic, obscene, indecent, lewd, vulgar or sexually offensive language, pictures or graphics or other communication that could reasonably be anticipated to cause a substantial disruption to the school environment.
   4. Employees shall not post content that negatively impacts their ability to perform their jobs.

Electronic Mail Violations. Forgery of electronic mail messages is prohibited. Reading, deleting, copying, or modifying the electronic mail of other users, without their permission is prohibited. Sending unsolicited junk mail, chain letters, political lobbying, transmitting obscene messages or pictures is prohibited.

Illegally Accessing or Hacking Violations. Illegally accessing or hacking and subsequent manipulation of information of private databases/systems is prohibited.

File/Data Violations. Deleting, examining, copying, or modifying files and/or data belonging to other users, without their permission is prohibited.

Copyright Violations. Downloading or using copyrighted information without following approved Dare County Schools procedures is prohibited.

System Interference/Alteration. Deliberate attempts to exceed, evade or change resource quotas (printing, downloading, storage) are prohibited. The deliberate causing of network congestion through mass consumption of system resources is prohibited.

Participation in Chat Rooms, Instant Messaging, and Newsgroups. Students and employees utilizing this district's electronic communications system, including access to the Internet, are prohibited in any chat room, Instant Messaging, or newsgroup accessed on the Internet, other than those approved and given access by the Technology Department.

Denial, Revocation, or Suspension of Access Privileges. With just cause, the System Administrator and/or building principal, may deny, revoke, or suspend Network/Internet access as required, pending an investigation.

Security

Reporting Security Problem. If knowledge of inappropriate material or a security problem on the Network/Internet is identified, the user should immediately notify his/her supervisor. The security problem should not be shared with others.

Impersonation. Attempts to log on to the Network/Internet impersonating a system administrator or Dare County Schools employee, student, or individual other than oneself, will result in revocation of the user's access to Network/Internet.

Other Security Risks. Any user identified as having had access privileges revoked or denied on another computer system may be denied access to the Dare County Schools Network/Internet.

Warning. Sites accessible via the Network/Internet may contain material that is illegal, defamatory, inaccurate or controversial. Dare County Schools makes every effort to limit access to objectionable material, however, controlling all such materials on the Network/Internet is impossible. With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting. The Dare County Schools Internet connection is the only system to be used in schools. No commercial Internet accounts may be used.

Disclaimer. This agreement applies to stand-alone computers as well as computers connected to the Network/Internet. Dare County Schools shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions, users' mistakes or negligence, or costs incurred by users. Dare County Schools shall not be responsible for ensuring the accuracy or usability of any information found on the internet.

The board is aware that there is information on the Internet that is not related to the educational program. The board also is aware that there is information and opportunities to communicate on subjects that are not suitable for school-age children and that many parents would find objectionable. The school district will take reasonable precautions to prevent students from having access to inappropriate materials, such as violence, nudity, obscenity or graphic language which does not serve a legitimate pedagogical concern. The school district will not limit access to the Internet for the purpose of restricting access to political ideas or social perspectives if the action is not rated simply by a school district official's disapproval of the ideas involved. However, the user is ultimately responsible for his or her activity on the Internet.

Legal Reference: U.S. Const. Amend. I; 17 U.S.C. 100 et seq.;Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; G.S. 115C-391, -325(e).

Cross Reference: Curriculum and Instructional Guides (policy 3115), Technology in the Educational Program (policy 3220), Copyright Complaint (policy 3230/7330), Standards of Expected Student Behavior (policy 4310), Public Records (policy 5070), Staff Responsibilities (policy 7300)

Adopted: July 25, 2003

Revised: October 13, 2009
August 4, 2014
August 21, 2017