The Internet is a unique opportunity to enhance instructional methods, appeal to different learning styles, and meet the educational goals of the board. Through the Internet, users can observe events as they occur around the world, interact with others on a variety of subjects, and acquire access to current and in-depth information.

As technological resources are developed and made available in the schools, their use should be integrated into the educational program. Technological resources should be used in teaching the North Carolina Standard Course of Study and in meeting the educational goals of the board. The curriculum committee should provide suggestions for using technological resources in the curriculum guides as provided in Board policy 3115, Curriculum and Instructional Guides. Teachers are encouraged to further incorporate the use of technological resources into their lesson plans.

This policy is designed to cover employees' use of the Martin County Schools' computer equipment, local-area and wide-area networks, and Internet access. The goal of the school system in providing this service is to facilitate resource sharing, innovation, and communication that are consistent with the educational objectives of the State of North Carolina and the Martin County Schools. Internet access includes the local, national, and international connections to: libraries, companies, agencies and businesses; discussion groups on a variety of subjects; information news services; and electronic mail communication.

I. EXPECTATIONS FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

1) The use of school system's technological resources, including access to the Internet, is a privilege, not a right. Individual users of the school system's technological resources are responsible for their behavior and communications when using those resources and must always comply with this policy. Responsible use of school system technological resources is use that is ethical, respectful, academically honest and supportive of student learning. Each user has the responsibility to respect others in the school community and on the Internet. General employee behavior standards, including those prescribed in applicable board policies, State and Federal Law and other regulations and school rules, apply to use of the Internet and other school technological resources.
2) No right of privacy exists in the use of technological resources. Users should not assume that files or communications created or transmitted using school system

technological resources or stored on services or hard drives of individual computers will be private. School system administrators or individuals designated by the superintendent may review files, monitor all communication, and intercept e-mail messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School system personnel shall monitor on-line activities of individuals who access technology resources via a school owned computer or school provided email.

3) Employees should be aware that the information and materials available on the Internet contain items that are illegal, defamatory, inaccurate, indecent or profane, and that on such a global network it is impossible to control all materials. Employees will be given the privilege to use the Internet along with the responsibility of using it properly. Martin County Schools' Internet access is coordinated through a complex association of government agencies as well as regional and state networks. The smooth operation of the network relies upon the proper conduct of those who use it. In general, this requires efficient, ethical and legal utilization of the network resources as well as adherence to school and Board of Education policies. If a user violates any of these provisions, his or her privilege to use the Internet will be terminated and future access could possibly be denied. In a case where laws or terms of employment are broken, additional consequences may follow, including disciplinary action up to and including termination.

II. RULES FOR USE

1) Internet access at school is intended to be used in preparation for class assignments, educational or career-development research, and personal research which does not violate the other provisions of this policy, in accordance with local and state educational objectives. Other uses of school access are to be considered inappropriate, and are not allowed.
2) The use of chat rooms by employees is strictly limited to those involving discussions of a professional and educational nature.
3) Users are expected to abide by the common rules of Network etiquette, as follows:
   1. Employees should use appropriate language and be polite in communications across the MCS network or Internet.
   2. Employees should not disrupt or attempt to disrupt the functioning of the MCS network communications or equipment in any manner, nor should they gain or

attempt to gain unauthorized access to the MCS network or any electronic records maintained by any other organization (hacking).

3. Employees should not reveal last names, ages, telephone numbers, or other personal identifying information about themselves or someone else to another person across the Internet or network.
4. Employees should not use another person's MCS network password or give their password to another employee or student for that person's use.
5. Employees should not access, publish, save, send or display indecent or profane images or text.
6. Employees should not violate copyright laws by copying files, programs, or other materials protected by copyright, or by failing to give credit to Internet sources used in their research.

4) The following activities and/or materials are specifically prohibited:
   1. Illegal, threatening, or defamatory activities prohibited by Board policy and North Carolina General Statutes (including, but not limited to, harassment, threats, cyberstalking, eavesdropping, and the use of misleading information or hate literature).
   2. The viewing, printing or sending of pornographic, obscene, or lewd materials.
   3. Vandalizing or attempting to vandalize hardware or software (including the creation or spread of viruses and hacking).
   4. Spamming (sending junk mail), advertising, or any commercial uses of the network.
   5. Wasting network resources, including excessive use of the MCS network, downloading files, and loading programs or games to the local workstation or the network without the prior approval of your network administrator.
   6. Copying for personal use software purchased by the school system.
   7. Using anonymous proxies or other measures to circumvent content filtering.
   8. Deleting files belonging to another user.
   9. Using school technological resources to express views or opinions purporting to be those of the school system.
   10. Demonstrating security problems (such as someone else's password, personal information, or access to restricted network software) to others or failure to notify the network administrator of the problem.

III. GENERAL PRINCIPLES

1. Employees should be aware that e-mail messages and any files stored in network directories or on the local hard drive(s) and any Internet activity may be considered public records under the North Carolina Public Records Act. These may be screened, supervised or viewed by school and system staff. Employees should not expect any privacy in these files.
2. Employees must delete e-mail from their inbox when no longer needed. If the email has been received from a source outside the Martin County Schools, then it must be archived before deletion. Emails sent by an employee must be promptly archived before deletion. Any email over 90 days old may be subject to deletion from the mail server. Employees must also keep their network folders emptied of non-crucial material, as any folders that become too large will not only slow down the networks' performance, but will be subject to deletion as well.
3. Home access to the Martin County Schools' network is subject to all the regulations and restrictions of this policy.
4. Martin County Schools does not guarantee the service it is providing, including delays, loss of data or connections, service interruptions and email deliveries. Martin County Schools does not control the material available on the Internet, and cannot be responsible for inaccurate data or offensive material encountered on the World Wide Web.
5. Martin County Schools will cooperate with law enforcement agencies on the investigation of any illegal activities involving internet/network use.

IV. PERSONAL WEBSITES

1. Students

Though school personnel generally do not monitor students' Internet activity conducted on non-school system devices during non-school hours, when the student's online behavior has a direct and immediate effect on school safety or maintaining order and discipline in the schools, the student may be disciplined in accordance with board policy.

1. Employees

Employees are to maintain an appropriate relationship with students at all times. Employees must block students from viewing personal information on employee personal websites or online networking profiles in order to prevent the possibility that students could view materials that are not age appropriate. If an employee creates and/or posts inappropriate content on a website or profile and it has a negative impact on the employee's ability to perform his or her job as it relates to working with students, the employee will be subject to discipline up to and including dismissal. This section applies to all employees and student teachers working in the school system.

Whether an employee chooses to personally participate in a blog, wiki, online social network or any other form of electronic online publishing or discussion, is his or her decision. However, material that employees post on social networks that is available to those in the school community must reflect the professional image applicable to the employee's position and not impair the employee's capacity to maintain the respect of students and parents/guardians or impair the employee's ability to serve as a role model for children. It is inappropriate to use email, text messaging, instant messaging, social networking tools, cell phones or any other forms of electronic communication to discuss with a student a matter that does not pertain to curriculum related activities. Personal websites, cell phones and any other form of personal electronic publishing by employees must not use photos or movies taken at school or contain pictures of students or staff.

Employees are prohibited from using electronic communications to establish personal relationships with students that are unprofessional and thereby inappropriate. Examples of unprofessional relationships include, but are not limited to: employee fraternizing or communicating with students as if employees and students were peers such as writing personal letters or emails, personally texting or calling students, or allowing students to make personal calls to them unrelated to homework, class work or other school related business, sending inappropriate pictures to students, discussing or revealing to students personal matters about their private lives or initiating students to do the same, and engaging in sexualized dialogue, whether in person, by phone, via the Internet or in writing. An employee who posts on social networking sites inappropriate personal information, including, but not limited to, provocative photographs, sexually explicit messages, abuse of alcohol, drugs or anything students are prohibited from doing, must understand that if students, parents or other employees obtain access to such information, the employee may be subject to disciplinary action after investigation by school and school system officials.

Employees must not use personal electronic communications or personal social networking tools to share confidential information about students or any specific information about students that would violate the Family Educational Rights and Privacy Act.

2. Volunteers

Volunteers are to maintain an appropriate relationship with students at all times. Volunteers are encouraged to block students from viewing personal information on volunteer personal websites or online networking profiles in order to prevent the possibility that students could view materials that are not age appropriate. An individual volunteer's relationship with the school system may be terminated if the volunteer engages in inappropriate online interaction with students.

V. DISCIPLINE ACTIONS

Any activities that violate this policy will make the user subject to disciplinary actions including revocation of the employee's network account and, depending upon the severity of the offense could result in termination of employment.

VI. LEGAL REFERENCES

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).

VII. LEGAL REFERENCES

All references to obscene, profane, offensive or illegal materials or matter are those defined in North Carolina General Statutes 14-190.1, 14-196.3, 14-202.3, 19-1.1, and19-12.

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: February 6, 2006
Revised: May 6, 2013