FACULTY AND STAFF RESPONSIBLE USE

It is expected that faculty and staff in Randolph County Schools will use Randolph County Schools' Internet accounts for instructional purposes. Faculty and staff members should maintain the highest ethical behavior in use of the Internet and should promote that behavior among students. It is the responsibility of faculty and staff members to:

1. Adhere to NC Student Information System (SIS) Password and Workstation Responsible Use Policy. (Regulation Code: (3225/4312/7320-R3)

2. Adhere to the Telecommunications Code of Ethics for the Randolph County Schools.

3. Supervise all students using Internet resources. It is essential that students using the Internet independently have an instructional staff member's permission to do so as well as signed Responsible Use Policy (RUP) from parents or guardians on file.

4. Points students toward worthwhile sites on the Internet that will amplify their knowledge and experience in curricular areas. Lesson preparation is required if students are to use Internet resources widely.

5. Ensure that all independent student users are informed annually of the guidelines of the Telecommunications Code of Ethics.

6. Follow the same criteria for Internet resources that are operable for all instructional materials under the Randolph County Schools' Selection of Instructional Materials Policy.

Users Full Name (Please Print)

____________________ ____________________ ____________________
(First) (Middle) (Last)

______________________________ ______________________________
(User Signature) (Date)

I have read, understand, and will abide by the Randolph County Schools' Technology Responsible Use Policy, Telecommunications Code of Ethics and NC Student Information System (SIS) Responsible Use Policy. I understand any violation of this policy and guidelines is unethical and will be subject to disciplinary action up to and including termination of employment or may constitute a criminal offense.

Regulation Code: 3225/4312/7320-R1 Technology Responsible Use

The Randolph County Schools offer students the opportunity to examine a broad range of opinions and ideas in the educational process, including the privilege to communicate and access information on the Internet and other electronic networks.

1. School officials must apply the same criterion of educational suitability used in the Randolph County Schools Selection Policy 3200 to the resources available through Internet and other electronic networks. Public complaints about Internet usage would follow procedures outlined in Board Policy 3210.

2. All of users of telecommunications will adhere to the TELECOMMUNICATIONS CODE OF ETHICS and NC Student Information System (SIS) Responsible Use Policy for Randolph County Schools.

3. A signed responsibility form from all instructional staff will be kept on file in the personnel file of each employee. A signed parental consent form will be on file before students are allowed individual access to the Internet and other electronic networks. This consent will be obtained for all students once in elementary, once in middle school, and once in high school.

4. Students are responsible for the educational, ethical, and legal use of the Internet and materials obtained through the Internet and other electronic networks.

5. The instructional staff in Randolph County Schools will use Internet accounts for instructional purposes. Instructional staff members should maintain the highest level of ethical behavior in the use of the Internet and should promote that behavior among students.

Randolph County Schools

Regulation Code: 3225/4312/7320-R2 Technology Responsible Use

TELECOMMUNICATIONS CODE OF ETHICS

1. The user shall accept the responsibility for all materials received and sent through telecommunications.

2. Users will limit their pursuit of information through electronic sources to curriculum-related activities.

3. Extensive personal use of the network is prohibited.

4. Any use of the network for commercial gain or profit is prohibited.

5. Inappropriate and/or illegal use of this technology may result in the loss of use, disciplinary action, and/or legal action. Messages relating to or in support of illegal or unethical activities will be reported to the appropriate authorities.

6. Users will use proper network etiquette. The use of inappropriate language or graphics, insults or harassment is not acceptable.

7. User ID/Passwords shall be kept confidential.

8. Electronic mail is not guaranteed to be private. Those who operate electronic mail systems have access to all mail and may report unethical or illegal activities to authorities.

9. Approval is required from the principal prior to subscribing to a newsgroup and/or listserv from the network. Participation in chat groups is prohibited.

10. Users are advised not to give out personal information such as a home address, phone number or last names to anyone via electronic networks.

11. Users will accept the responsibility of keeping copyrighted software of any kind from illegally entering the school over electronic networks. Observe copyright law when downloading information.

12. Appropriate bibliographic citations must be given for all information obtained via the Internet. It is unethical to plagiarize Internet resources just as it is unethical to plagiarize print resources.

13. Vandalism will result in immediate cancellation of user privileges and will require restitution.

Randolph County Schools

Regulation Code: 3225/4312/7320-R3 Technology Responsible Use

NC STUDENT INFORMATION SYSTEM (SIS) PASSWORD AND WORKSTATION RESPONSIBLE USE POLICY

The Randolph County Board of Education has the legal and ethical responsibility to collect, use and disseminates appropriate student information as one of its most important priorities. The legal aspects of the use of public school data are based upon several state and federal laws including the Uniform Education Reporting System (UERS) umbrella as required by GS 115C-12. Additionally, the Family Rights and Privacy Act (FERPA) as amended in 1996, mandate procedures for protecting the privacy of student data while acknowledging the necessity to collect it. North Carolina further defines the situations in which both student and education student data can (and cannot) be disclosed in GS 115C and State Board of Education Policy TCS-C-017.

The NC Student Information System (SIS) is the state's selected system for student accounting and collection and reporting of student information. The following will govern the use of NC Student Information System (SIS) in the Randolph County Schools.

1. Purpose

The purpose of this standard is to reduce unauthorized access to information within the NC Student Information System (SIS).

2. Application

All NC Student Information System (SIS) users are required to read and follow this policy concerning user identification (user ID), password protection, and workstation standards.

3. Background

This policy has been based on the guidelines of the Information Resource Management Commission (IRMC) policy set forth by the Department of Public Instruction while outlining specific guidelines for its own technology environment. The use of passwords in conjunction with unique user IDs is required in order to allow authorized access to the NC Student Information System (SIS) information. It is intended to prohibit the possibility of compromising student information and to maintain the integrity, accuracy, and confidentiality of the student data for the school district.

4. Scope

This policy applies to anyone using the NC Student Information System (SIS) application per State Board Policy TCS-C-018.

5. Policy - User ID and Password Standards

- Each user accessing the NC Student Information System (SIS) application shall be uniquely identified with an ID that is associated only with that user.
- No user shall allow another person to view or edit NC Student Information System (SIS) data using his/her user access.
- The LEA security administrator, or his/her designee, is responsible for promptly disabling the NC Student Information System (SIS) user ID upon termination of a user from the school or LEA or upon cessation of a user's need to access the NC Student Information System (SIS) system.
- Only authorized security administrators or help desk staff shall be allowed to enable a user ID.
- Passwords should not contain dictionary words or abbreviations.
- Passwords must be at least eight (8) characters in length.
- At no time should anyone from DPI call a user and request that user's password.
- Personal information such as social security numbers, drivers license numbers, etc. should not be inserted into email messages or other forms of electronic communication without proper encryption.
- If a password issue occurs when trying to login to the NC Student Information System (SIS), the user should contact the school data manager. Users should not try to contact NCDPI.
- LOG-IN INFORMATION, UID & PASSWORDS CANNOT BE SHARED WITH ANYONE. EACH USER IS PERSONALLY RESPONSIBLE FOR ALL DATA ENTRY UNDER HIS/HER NAME.

6. Workstation Security Standards

A. Users should not login using NC Student Information System (SIS) user identification to a public access computer. This includes, but is not limited to computer labs, cyber cafes, coffee shops, bookstores, libraries, etc.

B. Anti-virus software should be installed on each desktop computer, and designated staff shall make certain that the desktop has the most current anti-virus software and appropriate updates installed. Users should update the virus protection software weekly to avoid unwanted viruses or damage that can be caused by them.

C. NC Student Information System (SIS) passwords should be written or stored in clear text on or around the desktop systems.

D. Users should never leave the computer unattended while logged into NC Student Information System (SIS). The computer must be locked using the feature built into the software.

E. Only approved software should be installed on an NC Student Information System (SIS) -designated computer.

F. Browsers should be configured so that passwords for websites are not stored in the browser.

G. Users should watch for keystroke monitors. These are small devices, less than an inch in size, which can be plugged in between the keyboard cable and the CPU. They record every character typed (including passwords) and save them in a text file or send them to a remote user.

H. Workstation must be protected by a firewall.

I. Users must create a separate user profile for students to use the NC Student Information System (SIS) -designated computer.

J. Accessing NC Student Information System (SIS) from home will be permitted if the user can meet standards B, D, F, and H above.

7. Changing this policy

This policy may be modified at any time by the Randolph County Board of Education.

8. Enforcement

Enforcement of this policy will be handled by the Superintendent or his/her designee.

9. Areas of Responsibility

It is the responsibility of the Superintendent or his/her designee to ensure any changes to this policy are communicated to end users.

Randolph County Schools

Policy Code: 3225/4312/7320 Technology Responsible Use

The board provides its students and staff access to a variety of technological resources. These resources provide opportunities to enhance learning and improve communication within the school community and with the larger global community. Through the school system's technological resources, 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.

The board intends that students and employees benefit from these resources while remaining within the bounds of safe, legal and responsible use. Accordingly, the board establishes this policy to govern student and employee use of school system technological resources. This policy applies regardless of whether such use occurs on or off school system property, and it applies to all school system technological resources, including but not limited to computer networks and connections, the resources, tools and learning environments made available by or on the networks and all devices that connect to those networks.

A. EXPECTATIONS FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

The use of school system 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. 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. Users are expected to abide by the generally accepted rules of network etiquette. General student and employee behavior standards, including those prescribed in applicable board policies, the Code of Student Conduct and other regulations and school rules, apply to use of the Internet and other school technological resources.

In addition, anyone who uses school system computers or electronic devices or who accesses the school network or the Internet using school system resources must comply with the additional rules for responsible use listed in Section B, below. These rules are intended to clarify expectations for conduct but should not be construed as all-inclusive.

Before using the Internet, all students must be trained about appropriate online behavior as provided in policy 3226/4205, Internet Safety.

All students and employees must be informed annually of the requirements of this policy and the methods by which they may obtain a copy of this policy. Before using school system technological resources, students and employees must sign a statement indicating that they understand and will strictly comply with these requirements and acknowledging awareness that the school system uses monitoring systems to monitor and detect inappropriate use of technological resources. Failure to adhere to these requirements will result in disciplinary action, including revocation of user privileges. Willful misuse may result in disciplinary action and/or criminal prosecution under applicable state and federal law.

B. RULES FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

1. School system technological resources are provided for school-related purposes only. Acceptable uses of such technological resources are limited to responsible, efficient and legal activities that support learning and teaching. Use of school system technological resources for commercial gain or profit is prohibited. Student personal use of school system technological resources for amusement or entertainment is also prohibited. Because some incidental and occasional personal use by employees is inevitable, the board permits infrequent and brief personal use by employees so long as it occurs on personal time, does not interfere with school system business and is not otherwise prohibited by board policy or procedure.

2. Under no circumstance may software purchased by the school system be copied for personal use.

3. Students and employees must comply with all applicable laws, including those relating to copyrights and trademarks, confidential information, and public records. Any use that violates state or federal law is strictly prohibited. Plagiarism of Internet resources will be treated in the same manner as any other incidents of plagiarism, as stated in the Code of Student Conduct.

4. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally viewing, accessing, downloading, storing, printing or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages or other material that is obscene, defamatory, profane, pornographic, harassing, abusive or considered to be harmful to minors.

5. The use of anonymous proxies to circumvent content filtering is prohibited.

6. Users may not install or use any Internet-based file sharing program designed to facilitate sharing of copyrighted material.

7. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).

8. Users must respect the privacy of others. When using e-mail, chat rooms, blogs or other forms of electronic communication, students must not reveal personal identifying information, or information that is private or confidential, such as the home address or telephone number, credit or checking account information or

social security number of themselves or fellow students. For further information regarding what constitutes personal identifying information, see policy 4705/7825, Confidentiality of Personal Identifying Information. In addition, school employees must not disclose on school system websites or web pages or elsewhere on the Internet any personally identifiable, private or confidential information concerning students (including names, addresses or pictures) without the written permission of a parent or guardian or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA) or policy 4700, Student Records. Users also may not forward or post personal communications without the author's prior consent.

9. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks or data of any user connected to school system technological resources. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance. Users must scan any downloaded files for viruses.

10. Users may not create or introduce games, network communications programs or any foreign program or software onto any school system computer, electronic device or network without the express permission of the technology director or designee.

11. Users are prohibited from engaging in unauthorized or unlawful activities, such as "hacking" or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems or accounts.

12. Users are prohibited from using another individual's ID or password for any technological resource without permission from the individual. Students must also have permission from the teacher or other school official.

13. Users may not read, alter, change, block, execute or delete files or communications belonging to another user without the owner's express prior permission.

14. Employees shall not use passwords or user IDs for any data system (e.g., the state student information and instructional improvement system applications, time-keeping software, etc.) for an unauthorized or improper purpose.

15. If a user identifies a security problem on a technological resource, he or she must immediately notify a system administrator. Users must not demonstrate the problem to other users. Any user identified as a security risk will be denied access.

16. Teachers shall make reasonable efforts to supervise students' use of the Internet during instructional time.

17. Views may be expressed on the Internet or other technological resources as representing the view of the school system or part of the school system only with prior approval by the superintendent or designee.

C. RESTRICTED MATERIAL ON THE INTERNET

The Internet and electronic communications offer fluid environments in which students may access or be exposed to materials and information from diverse and rapidly changing sources, including some that may be harmful to students. The board recognizes that it is impossible to predict with certainty what information on the Internet students may access or obtain. Nevertheless school system personnel shall take reasonable precautions to prevent students from accessing material and information that is obscene, pornographic or otherwise harmful to minors, including violence, nudity, or graphic language that does not serve a legitimate pedagogical purpose. The superintendent shall ensure that technology protection measures are used as provided in policy 3226/4205, Internet Safety, and are disabled or minimized only when permitted by law and board policy. The board is not responsible for the content accessed by users who connect to the Internet via their personal mobile telephone technology (e.g., 3G, 4G service).

D. PARENTAL CONSENT

The board recognizes that parents of minors are responsible for setting and conveying the standards their children should follow when using media and information sources. Accordingly, before a student may independently access the Internet, the student's parent must be made aware of the possibility that the student could obtain access to inappropriate material while engaged in independent use of the Internet. The parent and student must consent to the student's independent access to the Internet and to monitoring of the student's internet activity and e-mail communication by school personnel.

In addition, in accordance with the board's goals and visions for technology, students may require accounts in third party systems for school related projects designed to assist students in mastering effective and proper online communications or to meet other educational goals. Parental permission will be obtained when necessary to create and manage such third party accounts.

E. PRIVACY

Students, employees, visitors, and other users have no expectation of privacy in anything they create, store, send, delete, receive, or display when using the school system's network, devices, Internet access, email system, or other technological resources owned or issued by the school system, whether the resources are used at school or elsewhere, and even if the use is personal purposes. Users should not assume that files or communications created, transmitted, or displayed using school system technological resources or stored on servers or on the storage mediums of individual devices will be private. The school system may, without notice, (1) monitor, track, and/or log network access, communications, and use; (2) monitor and allocate fileserver space; and (3) access, review, copy, store, delete or disclose the content of all user files, regardless of medium, the content of electronic mailboxes, and system outputs, such as printouts, for any lawful purpose. Such purposes may include, but are not limited to, maintaining system integrity, security, or functionality, ensuring compliance with board policy and applicable laws and regulations, protecting the school system from liability, and complying with the public records requests. School system personnel shall monitor online activities of individuals who access the Internet via a school-owned device.

F. USE OF PERSONAL TECHNOLOGY ON SCHOOL SYSTEM PROPERTY

Each principal may establish rules for his or her school site as to whether and how personal technology devices (including, but not limited to smart phones, tablets, laptops, etc.) may be used on campus. Students' devices are governed also by policy 4318, Use of Wireless Communication Devices. The school system assumes no responsibility for personal technology devices brought to school.

G. PERSONAL WEBSITES

The superintendent may use any means available 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 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 (see the student behavior policies in the 4300 series).

2. Employees

Employees' personal websites are subject to policy 7335, Employee Use of Social Media.

3. 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.

H. TEXTING

Employees, non-Randolph County School employed but support personnel (i.e. lay coaches, band coaches, boosters, club sponsors, etc.) and school volunteers should not send text messages to individual students. When text messaging is used for school-related matters, the following rules apply:

1. Employees, non-instructional support and school volunteers shall not send text messages to elementary and middle school students;

2. Employees, non-instructional support and school volunteers shall use group texting websites (such as "cel.ly" , "Remind 101") to communicate with high school students via text message;

3. Employees, non-instructional support and school volunteers must invite parents to join the group texting website;

4. Employees, non-instructional support and school volunteers may not communicate with high school students via text message unless the student's parent or guardian has provided a phone number for texting that is listed in the NC Student Information System/ HomeBase database; and

5. Employees, non-instructional support and school volunteers may only text high school students on the number listed in the NC Student Information System/Home Base database; and

6. Employees, non-instructional support and school volunteers must keep a record of all texts sent to and from students.

As a general rule, student record information protected by the Family Education Rights and Privacy ACT (FERPA) and personnel records confidential pursuant to state law should not be sent via email, text, or facsimile unless sent in a secure manner.

Legal References: U.S. Const. amend. I; Children's Internet Protection Act, 47 U.S.C. 254(h)(5); Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; 17 U.S.C. 101 *et seq.*; 20 U.S.C. 6777; G.S. 115C-325(e) (applicable to career status teachers), -325.4 (applicable to non-career status teachers)
Cross References: Curriculum and Instructional Guides (policy 3115), Technology in the Educational Program (policy 3220), Internet Safety (policy 3226/4205), Copyright Compliance (policy 3230/7330), Web Page Development (policy 3227/7322), Student Behavior Policies (all policies in the 4300 series), Student Records (policy 4700),

Confidentiality of Personal Identifying Information (policy 4705/7825), Public Records - Retention, Release and Disposition (policy 5070/7350), Use of Equipment, Materials and Supplies (policy 6520), Network Security (policy 6524), Staff Responsibilities (policy 7300), Employee Use of Social Media (policy 7335)

Administrative Rule: Yes

Exhibits Available: Yes

Adopted: February 26, 2001

Revised: November 18, 2002; November 9, 2009; November 19, 2012; September 16, 2013; July 21, 2014; February 23, 2015

Randolph County Schools