HR USE ONLY: _____

ECPPS STAFF TECHNOLOGY RESPONSIBLE USE

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 below. These rules are intended to clarify expectations for conduct but should not be construed as all-inclusive.

I acknowledge that I have read and understand the policies included in this document, including but not limited to: Policy Code: 3225/4312/7320 Technology Responsible Use, Policy Code: 3226/4205 Internet Safety, and Policy Code: Employee use of Social Media. I hereby agree to strictly comply with the terms and conditions of the above stated policies and rules - communicating over the network in a responsible manner while honoring all relevant laws and restrictions.

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 and tracking systems to track and recover lost or stolen equipment. Failure to adhere to these requirements will result in disciplinary action, including revocation of user privileges. Should I commit any violation, my access privileges may be revoked; I may be subject to disciplinary action, up to and including dismissal; and/or appropriate legal action. Willful misuse may result in criminal prosecution under applicable state and federal law.

I understand that if I do not sign this agreement, I will not be permitted to access ECPPS internet or email in school.

_____	_____	_____
Printed Staff Name	**Staff Signature**	**Date**

_____ _____

School

Implemented: April 27, 2015
Revised: August 9, 2016

RETURN TOP SHEET ONLY

ECPPS STAFF TECHNOLOGY RESPONSIBLE USE

Policy Code: 3225/4312/7320 Technology Responsible Use

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.

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 for 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 public records requests. School system personnel shall monitor online activities of individuals who access the Internet via a school-owned device.
By using the school system's network, Internet access, email system, devices, or other technological resources, individuals consent to have that use monitored by authorized school system personnel as described in this policy.

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.
Personal technology devices should not be connected to the school system's wired network

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).

Policy Code: 7335 Employee Use of Social Media

The board acknowledges that school employees may engage in the use of social media during their personal time. School employees who use social media for personal purposes must be mindful that they are responsible for their public conduct even when not acting in their capacities as school system employees. All school employees, including student teachers and independent contractors, shall comply with the requirements of this policy when using electronic social media for personal purposes. In addition, all school employees must comply with policy 4040/7310, Staff-Student Relations, when communicating with individual students through other electronic means, such as through voice, email, or text-messaging.

DEFINITIONS

1. Social Media

For the purposes of this policy, "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 policy, 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.

2. School-Controlled Social Media

"School-controlled social media" are social media networks, tools, or activities that are under the direct control and management of the school system and that create an archived audit trail.

3. Personal Social Media

"Personal social media" means any social media networks, tools, or activities that are not school-controlled.

SOCIAL MEDIA COMMUNICATIONS INVOLVING STUDENTS

Employees are to maintain professional relationships with students at all times in accordance with policies 4040/7310, Staff-Student Relations, and 7300, Staff Responsibilities. The use of electronic media for communicating with students and parents is an extension of the employee's workplace responsibilities. Accordingly, the board expects employees to use professional judgment when using social media or other electronic communications and to comply with the following.

1. All electronic communications with students who are currently enrolled in the school system must be school-related and within the scope of the employees' professional responsibilities, unless otherwise authorized by this policy or policy 4040/7310, Staff-Student Relations.
2. School employees may use only school-controlled social media to communicate directly with current students about school-related matters. (For information regarding communication with students through other forms of electronic communication, e.g., email or texts, see policy 4040/7310, Staff-Student Relations.)
3. Employees are prohibited from knowingly communicating with current students through personal social media without parental permission. An Internet posting on a personal social media website intended for a particular student will be considered a form of direct communication with that student in violation of this policy unless the parent has consented to the communication. However, an employee may communicate with a student using personal

social media to the extent the employee and student have a family relationship or other type of appropriate relationship which originated outside of the school setting. For example, an employee may have a relationship with a niece or nephew, a student who is the child of an adult friend, a student who is a friend of the employee's child, or a member or participant in the same civic, social, recreational, sport, or religious organization.
4. An employee seeking to utilize and/or establish a non-school-controlled social media website for instructional or other school-related purposes must have prior written approval from the principal and the superintendent or designee and must verify that the social media application's terms of service meet the requirements of policies 3220, Technology in the Educational Program, 3225/4312/7320, Technology Responsible Use, and 3227/7322, Web Page Development. If the website collects personal information from students under the age of 13, the use will not be approved unless the applicable requirements of the Children's Online Privacy Protection Act (COPPA) are met. The employee shall ensure that the website does not include or link to the employee's personal social media footprint. The site must be used for school-related purposes only.

EMPLOYEE PERSONAL USE OF SOCIAL MEDIA

The board respects the right of employees to use social media as a medium of self-expression on their personal time. As role models for the school system's students, however, 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. Further, school employees remain subject to applicable state and federal laws, board policies, administrative regulations, and the Code of Ethics for North Carolina Educators, even if communicating with others concerning personal and private matters. If an employee's use of social media interferes with the employee's ability to effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment.
Employees are responsible for the content on their social media sites, including content added by the employee, the employee's "friends," or members of the public who can access the employee's site, and for Web links on the employee's site. Employees shall take reasonable precautions, such as using available security settings, to manage students' access to the employee' personal information on social media websites and to prevent students from accessing materials that are not age-appropriate.
School employees are prohibited from accessing social networking websites for personal use during instructional time.

POSTING TO 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 not accept current students as "friends" or "followers" or otherwise connect with students on personal social media sites without parental permission, unless the employee and student have a family relationship or other type of appropriate relationship which originated outside of the school setting.
3. Employees shall not knowingly allow students access to their personal social media sites that discuss or portray sex, nudity, alcohol, or drug use or other behaviors associated with the employees' private lives that would be inappropriate to discuss with a student at school.
4. Employees may not knowingly grant students access to any portions of their personal social media sites that are not accessible to the general public without parental permission, unless the

employee and student have a family relationship or other type of appropriate relationship which originated outside of the school setting.
5. Employees shall be professional in all Internet postings related to or referencing the school system, students or their parents, and other employees.
6. 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.
7. Employees shall not use the school system's logo or other copyrighted material of the system on a personal social media site without express, written consent from the board.
8. Employees shall not post identifiable images of a student or student's family on a personal social media site without permission from the student and the student's parent or legal guardian. Employees may post such images on a school-controlled social media site only with prior permission of the employee's supervisor and in accordance with the requirements of federal and state privacy laws and policy 4700, Student Records.
9. Employees shall not use Internet postings to libel or defame the board, individual board members, students, or other school employees.
10. Employees shall not use Internet postings to harass, bully, or intimidate students or other employees in violation of policy 1710/4021/7230, Prohibition Against Discrimination, Harassment, and Bullying, or state and federal laws.
11. Employees shall not post content that negatively impacts their ability to perform their jobs.
12. Employees shall not use Internet postings to engage in any other conduct that violates board policy or administrative procedures or state and federal laws.

CONSEQUENCES

School system personnel shall monitor online activities of employees who access the Internet using school technological resources. Additionally, the superintendent or designee may periodically conduct public Internet searches to determine if an employee has engaged in conduct that violates this policy. Any employee who has been found by the superintendent to have violated this policy may be subject to disciplinary action, up to and including dismissal.