2018-2019
Technology Responsible Use Policy

Policy Code: 3225/4312/7320 Technology Responsible Use
Policy Code: 3226/4205 Internet Safety
AR Code: 3227/7322-R Web Page Development
Policy Code: 3230/7330 Copyright Compliance
Policy Code: 7335 Employee Use of Social Media
Regulation Code: 7335-R Approved Social Media Sites for Employee Use

Technology Responsible Use Agreement Form for Employees
Policy Code 3225-A, 3226, 3227, 3230, 4205, 4312, 7320, 7322-R, 7330, and 7335-R

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 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.

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 smartphones, 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.

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. 7131; 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)

Adopted:

Revised: December 6, 2016

Policy Code: 3226/4205 Internet Safety

A. INTRODUCTION

It is the policy of the board to: (a) prevent user access via its technological resources to, or transmission of, inappropriate material on the Internet or through electronic mail or other forms of direct electronic communications; (b) prevent unauthorized access to the Internet and devices or programs connected to or accessible through the Internet; (c) prevent other unlawful online activity; (d) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (e) comply with the Children's Internet Protection Act.

B. DEFINITIONS

1. Technology Protection Measure

The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors.

2. Harmful to Minors

The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

a. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

b. depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

c. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

3. Child Pornography

The term "child pornography" means any visual depiction, including any photograph, film, video picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

a. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

b. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

c. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

4. Sexual Act; Sexual Contact

The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.

5. Minor

For purposes of this policy, the term "minor" means any individual who has not attained the age of 17 years.

C. ACCESS TO INAPPROPRIATE MATERIAL

To the extent practical, technology protection measures (or "Internet filters") will be used to block or filter access to inappropriate information on the Internet and World Wide Web. Specifically, blocking will be applied to audio and visual depictions deemed obscene or to be child pornography or harmful to minors. Student access to other materials that are inappropriate to minors will also be restricted. The board has determined that audio or visual materials that depict violence, nudity, or graphic language that does not serve a legitimate pedagogical purpose are inappropriate for minors. The superintendent, in conjunction with a school technology and media advisory committee (see policy 3200, Selection of Instructional Materials), shall make a determination regarding what other matter or materials are inappropriate for minors. School system personnel may not restrict Internet access to ideas, perspectives, or viewpoints if the restriction is motivated solely by disapproval of the viewpoints involved.

A student or employee must immediately notify the appropriate school official if the student or employee believes that a website or web content that is available to students through the school system's Internet access is obscene, constitutes child pornography, is "harmful to minors" as defined by CIPA, or is otherwise inappropriate for students. Students must notify a teacher or the school principal; employees must notify the superintendent or designee.

Due to the dynamic nature of the Internet, sometimes Internet websites and web material that should not be restricted are blocked by the Internet filter. A student or employee who believes that a website or web content has been improperly blocked by the school system's filter should bring the website to the attention of the principal. The principal shall confer with the technology director to determine whether the site or content should be unblocked. The principal shall notify the student or teacher promptly of the decision. The decision may be appealed through the school system's grievance procedure. (See policies 1740/4010, Student and Parent Grievance Procedure, and 1750/7220, Grievance Procedure for Employees.) Subject to staff supervision, technology protection measures may be disabled during use by an adult for bona fide research or other lawful purposes.

D. INAPPROPRIATE NETWORK USAGE

All users of school system technological resources are expected to comply with the requirements established in policy 3225/4312/7320, Technology Responsible Use. In particular, users are prohibited from: (a) attempting to gain unauthorized access, including "hacking" and engaging in other similar unlawful activities; and (b) engaging in the unauthorized disclosure, use, or dissemination of personal identifying information regarding minors.

E. EDUCATION, SUPERVISION, AND MONITORING

To the extent practical, steps will be taken to promote the safety and security of users of the school system's online computer network, especially when they are using electronic mail, chat rooms, instant

messaging, and other forms of direct electronic communications. It is the responsibility of all school personnel to educate, supervise, and monitor usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures are the responsibility of the technology director or designated representatives.

The technology director or designated representatives shall provide age-appropriate training for students who use the school system's Internet services. The training provided will be designed to promote the school system's commitment to educating students in digital literacy and citizenship, including:

1. the standards and acceptable use of Internet services as set forth in policy 3225/4312/7320, Technology Responsible Use;

2. student safety with regard to safety on the Internet, appropriate behavior while online, including behavior on social networking websites and in chat rooms, and cyberbullying awareness and response; and

3. compliance with the E-rate requirements of the Children's Internet Protection Act.

Following receipt of this training, the student must acknowledge that he or she received the training, understood it, and will follow the provisions of policy 3225/4312/7320, Technology Responsible Use.

The superintendent shall develop any regulations needed to implement this policy and shall submit any certifications necessary to demonstrate compliance with this policy.

Legal References: Children's Internet Protection Act, 47 U.S.C. 254(h); Neighborhood Children's Internet Protection Act, 47 U.S.C. 254(l); Protecting Children in the 21st Century Act, 47 U.S.C. 254(h)
Cross References: Professional and Staff Development (policy 1610/7800), Student and Parent Grievance Procedure (policy 1740/4010), Grievance Procedure for Employees (policy 1750/7220), Technology in the Educational Program (policy 3220), Technology Responsible Use (policy 3225/4312/7320), School Improvement Plan (policy 3430), Use of Equipment, Materials, and Supplies (policy 6520), Network Security (policy 6524)

Adopted: May 16, 2017 at a public meeting, following normal public notice

Replaces: August 2, 2011

AR Code: 3227/7322-R Web Page Development

I. Applicability

This regulation applies to all system-related websites. A system-related website is defined as any Internet website or webpage that is established in one of the following ways: (1) by school system employees or students on behalf of the system; (2) by any school within the system; (3) by any school-sponsored club or organization within the system; or (4) by students as part of an educational assignment.

II. Responsibility for System-Related Websites

A. All System-Related Websites

Chief Technology Officer will serve as the school system's webmaster. The webmaster will oversee all system-related websites and may develop additional rules or guidelines governing the creation and maintenance of system-related websites.

B. Hyde County Schools Official Website

The superintendent retains ultimate control over the school system's official website; however, the superintendent delegates to the webmaster the responsibility for managing and maintaining the site. Only the superintendent, the webmaster, or school administrators designated by the webmaster may post material on the school system's official website. School system administrators who are assigned work on specific parts of the system website should consult with the webmaster when considering major changes in format or style or when dealing with content that could be sensitive or controversial.

C. Individual School Websites

Each principal has editorial control over and responsibility for the content of his or her individual school's official website, subject to the review of the superintendent and webmaster. The principal may appoint a staff member to serve as the school web manager. The school web manager shall assist the principal in ensuring that the school website adheres to the requirements of board policy, this regulation, and any other rules established by the webmaster. The principal may also appoint a website committee to advise the principal and school web manager regarding the content of the school's website. Only the principal or the school web manager or school administrators designated by the principal may post material on the school website. School administrators who are assigned work on specific parts of the school website should consult with the principal when considering major changes in format or style or when dealing with content that could be sensitive or controversial.

D. Class Websites

Teachers will be provided the opportunity to create individual class websites accessible through the school's website. The teacher has editorial control over and responsibility for the content of his or her class website, subject to review by the principal, the school web manager, the superintendent, and webmaster.

Before a teacher may create a class website, the teacher must annually complete the Hyde County Schools Class Module located in Canvas. Teachers must understand and agree to abide by all rules and requirements in board policy and this regulation and any other rules established by the principal, school web manager, superintendent, or webmaster regarding web page creation and maintenance.

E. Student Web Pages

With the knowledge and written consent of a student's parent or guardian, a teacher may allow a student to create a web page within or linked from the teacher's website only for the following instructional purposes: (1) to teach a student how to create or maintain a web page or (2) to facilitate a student's work on school assignments or research projects. No student pages may be posted or made accessible to the general public until approved by the principal or designee.

III. Formatting and Style of System-Related Websites

A. Page Appearance

All pages on a system-related website should be easy to navigate, be aesthetically pleasing, and not look overcrowded. All pages must adhere to formatting and style standards developed by the webmaster.

Graphics used must be appropriate to the school and should be of a size that will download quickly into a web browser. Large downloadable files, like video and music files, should not be included on school-related websites as they use large amounts of bandwidths.

"Under Construction" messages should not be used on the website. The page should be constructed before it is posted. If an "Under Construction" message is necessary, it should not be used on a page for longer than two weeks.

B. Writing Style

The information on system-related websites should be written in clear, plain language and should take into consideration the literacy and knowledge levels of the students, parents, and community members who will be viewing the website. The information should be grammatically correct and should not contain spelling or punctuation errors. Use of underlining should be avoided as underlined words can look like hyperlinks to the viewer.

IV. Content Standards for System-Related Websites

A. Purpose

1. System-related websites are closed forums for expression. The purposes of system-related websites are to disseminate curriculum-related information; to present the public with information about the system, its schools, and its programs; and to provide the community with each school or department's mission, contact information, activities, organizational format, and instructional program.

2. Any information presented on system-related websites should represent the official position of the school system and may not be false, misleading, illegal, obscene, defamatory, profane, pornographic, harassing, abusive, or considered harmful to minors.

3. System-related websites may not be used to promote personal beliefs, views, or opinions or to endorse political parties or candidates. The superintendent may authorize a principal to allow an exception to this rule for student-created websites that are part of a class assignment or project.

4. Use of system-related websites for advertising or personal commercial gain or profit is prohibited.

5. Any information display that is contrary to the purposes described here may be removed without notice by the superintendent or webmaster.

B. Accuracy

All information on a system-related website should be accurate, verifiable, and current.

C. Standard Information

With the exception of student webpages, each webpage in a system-related website must include the name and email address of the webpage's author and the date produced or last revised. Student web pages must contain the name and email address of the teacher of the webpage's author and the date produced or last revised.

D. Copyright Laws

No information or graphics may be posted on system-related websites in violation of any copyright laws or policy 3230/7330, Copyright Compliance. Copyright permission must be obtained for the use of any copyrighted material unless use is permitted as "fair use" under federal law. The Instructional Technology Facilitator and Media Specialist are responsible for maintaining copies of permission granted for the use of copyrighted material.

E. Personal Information

The safety of students and employees must be considered when constructing system-related websites. To protect the safety of students and employees, the following precautions must be taken:

1. home addresses and telephone numbers will not be listed;

2. student e-mail addresses will not be listed; and

3. photographs of students and student work will be used only with appropriate parental permission and/or as approved for release as directory information under policy 4700, Student Records, and will include only the student's first name, with no other information about the student.

The principal or Instructional Technology Department is responsible for maintaining records of permission granted for the release of information.

F. Specific Content on School System's Official Website

1. Contact Information

The school system's official website will provide contact information and other general information about the school system, including school system department phone numbers and fax numbers, the administrative office address, and the e-mail addresses of school system administrators.

2. Board Information

The school system's official website will include information about the board, such as the following.

- board member names, districts, biographies, pictures, and contact information
- board calendar
- board meeting notices and agendas
- board meeting minutes
- board policy manual
- board resolutions
- board committee information, including agendas and materials
- board advisory council information
- budget information

3. Mandatory Information

The school system's official website will display all information required by law or board policy including:

a. the overall school performance score and grade earned by each school in the school system for the current and previous four school years as required by G.S. 115C-47(58);

b. reading proficiency information about third-grade students as required by G.S. 115C-83.10;

c. information on state fund expenditures as required by G.S. 115C-105.25(c);

d. when a Title I school is identified for improvement, corrective action, or restructuring, information regarding supplemental services and public school choice as required by federal regulations and described in policy 1320/3560, Title I Parent Involvement; and

e. policy 1710/4021/7230, Prohibition Against Discrimination, Harassment, and Bullying, as required by that policy.

4. Other Information

Examples of additional types of information that may be provided on the school system's official website include, but are not limited to, the following.

- greeting message
- school system history
- lists of the schools in the school system and links to their websites
- information about departments and programs
- curriculum information
- promotion standards
- testing information
- the types of personally identifiable information the school system has designated as directory information and opportunities for parents to opt-out of disclosure of such information
- data collection and privacy practices
- statements of nondiscrimination
- grievance procedures
- calendars
- upcoming events
- news and announcements, including school delays and closings
- lunch menus
- Code of Student Conduct
- administrative rules, regulations, and procedures
- notifications and forms
- student assignment plan
- student awards
- employment information
- staff or school recognition
- staff resources
- links as described in Section V

G. Specific Content on School Websites

1. Contact Information

A school website must provide contact information and other general information about the school, including the school's name, phone number, fax number, grade levels, and address, the principal's name, and the e-mail addresses of the school administrative team. The website also may contain a staff directory.

2. Mandatory Notifications

The school website will display all information required by law including:

1. the school's consolidated plan as required by G.S. 115C-12(19);

2. names of the members of the school improvement team, their positions, and the date of their election to the school improvement team as required by G.S. 115C-105.27(a2); and

3. the school improvement plan, except for the school safety components of the plan as required by G.S. 115C-105.27(a2).

3. Other Information

The following is a non-exhaustive list of additional types of information that a school website could include.

- greeting message
- school history
- academic program descriptions
- curriculum information
- promotion standards
- support services information
- school calendar
- upcoming events
- news and announcements
- lunch menu
- school clubs and organizations information
- student handbook and other school rules
- parental notifications and forms
- student awards
- staff recognition
- staff resources
- links to class websites and other links as described in Section V

H. Specific Content on Class Websites

1. Contact Information

Each class website must clearly state the teacher's name, the grade level and/or course title, and the name, address, and phone number of the school. Teachers are encouraged to provide their school email address on the website, as well as information regarding how to contact the teacher and how to set up a parent-teacher conference.

2. Class Information

The following are examples of the types of class information that may be displayed on the class website.

- course syllabus
- class calendar
- daily or weekly class schedules
- announcements
- behavior expectations
- academic expectations
- grading policies
- homework or other class assignments
- enrichment materials

- newsletters, parental notifications, and forms
- biographical information about the teacher

3. Links

A class website will contain internal links as described in subsection V.A. Subject to the requirements of subsection V.B, a class website may include links to external websites that contain:

- educational online games and activities for students
- scholarly articles
- other reputable reference materials.

The teacher should periodically check external links for accuracy and appropriateness of content.

4. Student Work

The class website may include general descriptions of work completed in the classroom throughout the year but may not include descriptions of a specific student's work without consent of the student's parent. Student works may not be published to the website without parental consent. Any published student work must be accompanied by notice that redistribution or reuse without consent of the student is prohibited. Any photographs of student work posted must comply with the requirements described in subsection IV.E.

V. Links

A. Internal Links

Each page of a system-related website must include a reference and hyperlink to the website home page and to the school system's official website homepage, if different.

All system-related websites must include a link to policy 3227/7322, Web Page Development, and to policy 3225/4312/7320, Technology Responsible Use. In addition, each class website must provide a reference and hyperlink to the school's website.

B. External Links

The superintendent, webmaster, principals, and school web managers have editorial control over and responsibility for including links on a system-related website to other sites on the Internet that are appropriate to the mission of the school system.

1. Approval of Links

Links to external sites on the school system's official website must be approved by the webmaster and are subject to review by the superintendent. Links to external sites on a school website, class website, or student page must be approved by the school web manager and the principal.

If required, the webmaster or web manager must obtain permission from external websites before links are established from any system-related website to external websites. To the extent possible, school personnel shall determine the extent to which a secondary site is linked to other sites on the Internet and whether such sites are appropriate for access through system-related websites.

2. Disclaimer Statement

Since the school system cannot control the content of other sites on the Internet and their linkages, the following disclaimer statement must be inserted in a prominent position on the school system's official website, on each school's website, and on other system-related websites that contain links to other websites or that are not system-related websites:

The school system retains control over what links will be placed on system-related websites; however, the linked sites themselves are not under the control of the school system, its agents, or its employees. The school system is not responsible for the contents of any linked site, any link contained in a linked site, or any changes or updates to such sites. The school system provides links as a convenience, and the inclusion of any link does not imply endorsement of the site by the school system. The school system reserves the right to remove or restrict any links.

3. Ongoing Review of Links

The webmaster and school web managers must periodically check external links for accuracy and appropriateness of content. School employees must report any inappropriate links to the web manager.

4. Impermissible External Links

System-related websites may not contain links to personal websites or web pages of students or employees or lists of personal websites or web pages.

Issued by the Superintendent: February 23, 2017
Reviewed:
Revised:

Policy Code: 3230/7330 Copyright Compliance

The board recognizes and supports the limitations on unauthorized duplication and use of copyrighted materials. The board does not condone any infringement on the property rights of copyright owners.

Employees, students and visitors are prohibited from the use or duplication of any copyright materials not allowed by copyright law, fair use guidelines sanctioned by Congress, licenses or contractual agreements. Willful or serious violations also are considered to be in violation of expected standards of behavior for employees and students and may result in disciplinary action in accordance with board policy.

A. FAIR USE

1. Unless allowed as "fair use" under federal law, permission must be acquired from the copyright owner prior to copying copyrighted material. Fair use is based on the following standards:
   a. the purpose and character of the use;
   b. the nature of the copyrighted work;
   c. the amount of and the substantiality of the portion used in relation to the copyrighted work as a whole; and
   d. the effect of the use upon the potential market for, or value of, the copyrighted work.
2. The superintendent or designee shall provide information and training to personnel and students, as appropriate, on the fair use of copyrighted materials, including in the following circumstances:
   a. single and multiple copying for instructional purposes;
   b. copying for performances and displays;
   c. off-air recording of copyrighted programs;
   d. use of "for home use only" videotapes or DVDs;
   e. computer software;
   f. copyrighted materials on the Internet and on-line databases; and
   g. reproduction and loan of copyrighted materials by school media centers.

B. BUDGET

The budget recommended by the superintendent to the board must include sufficient funds for purchasing copyrighted materials as a necessary budget expense.

Legal References: 17 U.S.C. 101, 102, 106, 108, 110, 117

Cross References: Technology in the Educational Program (policy 3220), Technology Acceptable Use (policy 3225/4312/7320), Integrity and Civility (policy 4310), Network Security (policy 6524), Staff Responsibilities (policy 7300), Budget Planning and Adoption (policy 8100)

Adopted: August 2, 2011

Policy Code: 7335 Employee Use of Social Media

The board recognizes the importance of incorporating current technology tools, including new methods of electronic communication, into the classroom to enhance student learning. It further recognizes the importance of employees, students, and parents engaging, learning, collaborating, and sharing in digital environments as part of 21st Century learning. The board strives to ensure that electronic communication tools incorporated into the school curriculum are used responsibly and safely. As practicable, the board will provide access to secure social media tools and board approved technologies for use during instructional time and for school-sponsored activities in accordance with policies 3220, Technology in the Educational Program, and 3225/4312/7320, Technology Responsible Use.

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.

A. 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.

B. 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 employee's 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.

C. 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 employees' 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.

D. 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 employee's 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.

E. 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.

The superintendent shall establish and communicate to employees guidelines that are consistent with this policy.

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); 16 N.C.A.C. 6C .0601, .0602; State Board of Education Policy NCAC-6C-0601

Cross References: Prohibition Against Discrimination, Harassment, and Bullying (policy 1710/4021/7230), Technology in the Educational Program (policy 3220), Technology Responsible Use (policy 3225/4312/7320), Web Page Development (policy 3227/7322), Copyright Compliance (policy 3230/7330), Staff-Student Relations (policy 4040/7310), Student Records (policy 4700), Staff Responsibilities (policy 7300)

Adopted: January 31, 2012

Revised: May 16, 2017

Regulation Code: 7335-R Approved Social Media Sites for Employee Use

The board recognizes the importance of incorporating current technology tools, including new methods of electronic communication, into the classroom to enhance student learning. It further recognizes the importance of employees, students and parents engaging, learning, collaborating and sharing in digital

environments as part of 21st Century learning. The board strives to ensure that electronic communication tools incorporated into the school curriculum are used responsibly and safely. As practicable, the board will provide access to secure social media tools and board approved technologies for use during instructional time and for school-sponsored activities in accordance with policies 3220, Technology in the Educational Program, and 3225/4312/7320, Technology Responsible Use.

All electronic communications with students who are currently enrolled in the school system must be school-related and within the scope of employee's professional responsibilities, unless otherwise authorized by policy 7335, Employee Use of Social Media. School personnel may use only school-controlled technological resources and social media tools to communicate directly with students or to comment on student matters through use of the Internet. An employee seeking to utilize and/or establish other non-school-controlled social media website for instructional or other school-related purposes must have prior written approval from the superintendent or designee and principal and meet any applicable requirements of policies 3220, Technology in the Educational Program, 3225/4312/7320, Technology Responsible Use, and 3227/7322, Web Page Development.

Schools and departments are allowed to have one official Facebook Page. It is managed and maintained by the administrator or his/her designee. It should NOT be set up under an employee's personal or school e-mail address. It should be created under a generic Gmail account for the school (example: ccs28306@gmail.com). If there are groups/clubs at the school that want to have a separate Facebook page, it must be approved by the principal and must be monitored by the school. The purpose of the page is to only share information, not to have a two-way conversation with visitors to the page. This also applies to Twitter. Both accounts are used to push out information, not to start a two-way conversation with the public.

In all cases, the school/teacher/administrator/pagemanager is responsible for making sure students DO NOT HAVE A REFUSAL OF PERMISSION FORM on file at the school.

All approved social media sites and their descriptions will be posted on the website of the Curriculum Department. An advisory group of administrators and teachers will be responsible for maintaining the list and reviewing possible sites. A designated administrator from the curriculum and technology departments will co-chair the committee.

Approved: By the Superintendent January 22, 2013.

Revised: May 15, 2017

EMPLOYEE TECHNOLOGY RESPONSIBLE USE AGREEMENT
***Policy Code* 3225-A, 3226, 3227, 3230, 4205, 4312, 7320, 7322-R, 7330, and 7335-R**

Each employee must sign this Agreement as a condition for using the School Division's computer system.

Prior to signing this Agreement, read Policies 3225, 3226, 3227, 3230, 4205, 4312, 7320, 7322, 7330, 7335, and 7335-R that are found under the School Board of Education Tab on the Division's webpage. If you have any questions about these policies, contact your supervisor or your principal.

I understand and agree to abide by the School Division's Technology Responsible Use Policy and all other policies referenced in the above paragraph. I understand that the School Division may access and monitor my use of the computer system, including my use of the Internet, e-mail, downloaded material, without prior notice to me. I further understand that should I violate the Acceptable Use Policy or any of the policies in the above paragraph, my computer system privileges may be revoked and disciplinary action and/or legal action may be taken against me.

Printed Name of Employee _____

Signature of Employee_____Date_____

PARENT/STUDENT TECHNOLOGY RESPONSIBLE USE AGREEMENT

***Policy Code* 3225-A, 3226, 3227, 3230, 4205, 4312, 7320, 7322-R, 7330, and 7335-R**

Each student and his or her parent/guardian must sign this Agreement before being permitted to use the School Division's computer system. Read this Agreement carefully before signing.

Prior to signing this Agreement, read Policies **3225-A, 3226, 3227, 3230, 4205, 4312, 7320, 7322-R, 7330, 7335, 7335-R** that are found under the school Board of Education Tab on the Division's webpage. If you have any questions about these policies, contact your supervisor or your student's principal.

I understand and agree to abide by the School Division's Technology Responsible Use Policy and all other policies referenced in the above paragraph. I understand that the School Division may access and monitor my use of the computer system, including my use of the Internet, e-mail, downloaded material, without prior notice to me. I further understand that should I violate the Acceptable Use Policy or any of the policies in the above paragraph, my computer system privileges may be revoked and disciplinary action and/or legal action may be taken against me.

Printed Name of Student_____

Signature of Student_____Date_____

I have read this Agreement and Policies **3225-A, 3226, 3227, 3230, 4205, 4312, 7320, 7322-R, 7330, and 7335-R**. I understand that access to the computer system is intended for educational purposes and the Hyde County School Division has taken precautions to eliminate inappropriate material. I also recognize, however, that it is impossible for the School Division to restrict access to all inappropriate material and I will not hold the School Division responsible for information acquired on the computer system. I have discussed the terms of this agreement and policies with my student.

I grant permission for my student to use the computer system in accordance with Hyde County School District policies and for the School Division to issue an account for my student.

Printed Name of Parent/Guardian _____

Signature of Parent/Guardian _____ Date _____