Regulation

Acceptable Computer System Use

The Amelia County Public Schools (the "school division" or "division") values the impact technology has on personal growth and academic achievement. This regulation is a guide to ensure that the computer system in each of our schools is used as a safe and secure learning platform. This regulation shall cover all individuals who use or may have access to the school division's computer system, including students, teachers/staff, and guests of the school division.

Definitions

For the purposes of this regulation:

1. "Computer system" shall have the same definition as provided in School Board policy GAB/IIBEA, Acceptable Use Policy.

2. "Computer network" means internet, intranet, or other online access, either through a wired or wireless connection, to the school division's computer system or the World Wide Web.

3. "Credentials" are a set of unique identifiers to gain access to services on the computer system or network. "Credentials" include usernames, passwords, and potentially bio-metric identification systems such as fingerprint scanners.

4. "Devices" are computing or other electronic devices, including electronic handheld gaming devices, iPods or other MP3 players, iPads or other tablets, smart phones, laptops, personal computers, printers, tape drives, optical devices, USB drives, and other devices that may be able to access the division's computer network

5. "External devices" are computing or other electronic devices owned by students, their families, teachers/staff, or guests of the school division. This regulation covers how these devices may or may not be used on the division's computer network.

6. "Social networking" means the use of dedicated websites or other online services to communicate formally or informally with other members of the website or online service by posting messages, photographs, or other forms of communication (examples include Twitter, Facebook, Edmodo, AOL Instant Messaging, etc.). This regulation provides guidelines for the use of social networks for staff.

Please contact the school division technology staff for clarification on technical terms used in this regulation or for the names of services referenced within (Google Apps, Edmodo, etc.).

Guidelines

The school division will monitor user data and computer network access for both division-owned devices and external devices. The school division makes no guarantee for network access for external devices. Individuals who wish to connect external devices to the division's computer network must first obtain authorization and credentials for network access.

Violations of any policies, regulations, or school rules involving the use of external devices connected to the division's computer system or network may result in the loss of use of the device on school grounds and/or may subject the individual to any applicable disciplinary action. The division reserves the right to confiscate and inspect any external-device connected to the computer system or network if there is a reasonable suspicion of a violation of School Board policies, regulations, school rules, or other misconduct while using the external-device.

Educational uses of the computer system take precedence over non-educational uses such as entertainment, videos, and gaming.

School-owned devices may be audited by the Division Superintendent or designee at any time.

Purpose

The primary use of the computer system must be for educational purposes. Examples of educational purposes include:

- Learning assessment and testing;
- Media creation (written reports, podcasts, videos, artwork, etc.);
- Skills practice (educational games, informal assessment);
- Communication (class discussions, journal writing);
- Accessing information (research, webquests, reading); and
- Publishing original thoughts and ideas (blogs, webpages, videos).

Access

Any individual permitted to access the computer system shall be provided one or more unique credential(s) by the school division. Credentials are required to access individual computers, certain network services, online services, and other aspects of the computer system. Credentials shall not be divulged to others. Compromised credentials must be reported immediately to the school division's technology staff. Use of another individual's credential to access the computer system is strictly prohibited.

The school division may offer e-mail or other web services accounts to staff. These accounts must be used for school division business only and not for private communication.

The school division may permit the appropriate use of the computer network by students. This is a privilege that may be suspended if students engage in any of the following prohibited behaviors.

Prohibited Behaviors

The following behaviors do not support the educational mission of the school division and are, therefore, prohibited:

- Trespassing, Theft and Intrusion;
- Cyberbullying and harassment;
- Use of or access to Impermissible Software or Other Inappropriate Content;
- Divulgence of Confidential Student Information;
- Excessive and Impermissible Uses of Space and Storage; and
- Cheating.

Trespassing, Theft, and Intrusion include:

- Touching an electronic device without express permission of the owner.
- Use or manipulation of another person's user account.
- Accessing another person's files or resources.
- Accessing areas of the network for which an individual has not been given permission to access.
- Utilization of external network "hotspots" or access points inside school buildings without prior approval by school administration.
- Illegally downloading materials (e.g. cracked software, pirated music or movies, copyright-protected media) or intellectual property.
- Peer to peer file sharing (Bit Torrent, etc.).
- Spamming, hacking, hawking, or trolling.
- Sending or accessing content not directly associated with educational research, academic instruction, or school division business.
- Deliberately or negligently spreading viruses, malware, or spyware.
- Impermissibly attempting to access any aspects of the computer system.
- Private or non-school division profit ventures or fundraising via the computer system. Prohibited conduct includes but is not limited to using the email system to advertise for personal goods or services for sale or rent.

Cyberbulling and Harassment include:

- Bullying, harassment, threats, or intimidate another person via the computer system.
- Posting or sending messages, pictures, sounds, or video that is obscene, rude, harassing, or insulting to anyone.

Impermissible Software and Other Inappropriate Content include:

- Downloading and loading of any game, video, or music file on any computer system device that you have not paid for or that you do not have the right to use.
- Sending, receiving, viewing, or downloading illegal material via the Internet.
- Accessing material that the school division deems to be harmful to juveniles, including explicit or, obscene material and material that is otherwise inappropriate for minors.
- Online chats or playing music/videos without express permission.
- Taking or posting pictures of others without asking and receiving their permission.

.

Divulgence of Confidential Student Information

- Communication about or access to confidential student information shall meet the standards and requirements set forth in POLICIES JO and JOA.
- Confidential student information shall not otherwise be divulged via the computer system.

Excessive and Impermissible Uses of Space and Storage include:

- Excessive occupation of bandwidth on the computer system by downloading movies, music, pictures, or by playing online games not directly connected to educational research, academic instruction or school division business.
- Storage of music, movies, pictures, or files on the computer system not connected to educational research, academic instruction or school division business.
- Storage of personal files on the computer system.

Cheating

- Plagiarism via the computer system.
- Use of the computer system to compromise the integrity of assessments via impermissible research.

Social Networking Guidelines for Staff

Communications via the computer system between employees, volunteers, and individual students must be transparent, accessible to supervisors and parents, and professional in content and tone. The division believes this transparency in communication is vital for maintaining an open and safe environment for students. Employees are prohibited from the non-educational or non-job specific use of social networks (e.g. Facebook, Twitter, Pinterest, Google+, etc.) during contract hours. Such permitted use must be directly related to an employee's job function (s) and a supervisor may restrict an employee's use of social networks if the use is believed to negatively impact an employee's job performance and/or violate school board policies or regulations.

As with in-person communications, educators and volunteers must avoid appearances of impropriety and refrain from inappropriate electronic communications with students. Factors that may be considered in determining whether an electronic communication is inappropriate include, but are not limited to:

- The subject, content, purpose, authorization, timing and frequency of the communication;
- Whether there was an attempt to conceal the communication from supervisors and/or parents;
- Whether the communication could be reasonably interpreted as soliciting sexual contact or a romantic relationship;
- Whether the communication was sexually explicit; and
- Whether the communication involves discussion promoting illegal activity, including the use of controlled substances.

Communications between students and division staff and volunteers regarding school division business **shall be limited** to channels controlled by the school division. These include:

- Division e-mail accounts,
- Division telephone (school telephone), and
- Division educational online or cloud-based services.

Communications with students over social networks and through personal computing devices is discouraged and considered outside of official school business. Communications via these means is acceptable if the relationship between school personnel and volunteers with students has been appropriately established before the school relationship (i.e., the employee or volunteer is a relative, a family friend, or mentor).

Monitoring and Filtering

The Division Superintendent, in consultation with the Supervisor of Technology and/or Systems Administrator, will select and institute a technology protection measure to filter or block Internet access to

(a) child pornography as set out in Va. Code § 18.2-374.1:1 or as defined in 18 U.S.C. § 2256;

(b) obscenity as defined by Va. Code § 18.2-372 or 18 U.S.C. § 1460; and

(c) material that the school division deems to be harmful to juveniles as defined in Va.

Code § 18.2-390, material that is harmful to minors as defined in 47 U.S.C. § 254(h)(7)(G), and material that is otherwise inappropriate for minors;

Sanctions for Non-Compliance with This Regulation

For students:

- Withdrawal of privileges including network access;
- Confiscation of personal device used inappropriately;
- Withdrawal of the right to bring personal devices on school premises; and/or
- Payment for willful damage to the computer system.
- For serious breaches of these guidelines, incidents will be handled following the school division's discipline procedures, which can include suspension, expulsion, and involvement of law enforcement.

For teachers and staff:

- Documentation of infraction in personnel file;
- Payment for willful damage to the computer system; and/or
- For serious breaches of these guidelines, incidents will be processed as a personnel matter, which can include termination, and involvement of law enforcement and/or child protective services.

For guests:

- Restriction from having access to the computer system; and/or
- Payment for willful damage to the computer system.
- For serious breaches of these guidelines, the guest may be banned from use and incidents may be reported to law enforcement agencies and/or child protective services.

Liability

The school division makes no warranties for the computer system it provides and denies any responsibility for the accuracy or quality of information obtained through the computer system. The school division shall not be responsible for any damages to the user from use of the computer system, including loss of data, non-delivery or missed delivery of information, or service interruptions. The user agrees to indemnify the school division for any losses, costs, or damages incurred by the school division relating to or arising out of any violation of this regulation.

Revised: August 13, 2013

ACCEPTABLE COMPUTER SYSTEM USE AGREEMENT

Each employee must sign this Agreement as a condition for using the School Division's computer system. 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 Policy GAB/IIBEA and Regulation GAB-R/IIBEA-R, Acceptable Computer System Use. If you have any questions about this policy or regulation, contact your supervisor or your student's principal.

I understand and agree to abide by the School Division's Acceptable Computer System Use Policy and Regulation. I understand that the School Division may access, monitor, and archive my use of the computer system, including my use of the internet, e-mail and downloaded material, without prior notice to me. I further understand that should I violate the Acceptable Use Policy or Regulation, my computer system privileges may be revoked and disciplinary action and/or legal action may be taken against me.

Student/Employee Signature _____ Date_____

I have read this Agreement and Policy GAB/IIBEA and Regulation GAB-R/IIBEA-R. I understand that access to the computer system is intended for educational purposes and the Amelia 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, policy, and regulation with my student.

I grant permission for my student to use the computer system in accordance with Amelia County School Division's policies and regulations and for the School Division to issue an account for my student.

Parent/Guardian Signature _____Date _____

Parent/Guardian Name _____
(Please Print)