

ACCEPTABLE COMPUTER SYSTEM USE

All use of the Allegheny County School Division's computer system shall be consistent with the School Board's goal of promoting educational excellence by facilitating resource sharing, innovation and communication. The term computer system includes, but is not limited to, hardware, software, data, communication lines and devices, terminals, printers, CD-ROM devices, tape or flash drives, servers, mainframe and personal computers, tablets, cellular phones, smart phones, the internet and any other internal or external network.

Computer System Use-Terms and Conditions:

1. **Acceptable Use.** Access to the Division's computer system shall be (1) for the purposes of education or research and be consistent with the educational objectives of the Division or (2) for legitimate school business.

2. **Privilege.** The use of the Division's computer system is a privilege, not a right.

3. **Unacceptable Use.** Each user is responsible for his or her actions on the computer system. Prohibited conduct includes but is not limited to:
 - using the network for any illegal or unauthorized activity, including violation of copyright or contracts, or transmitting any material in violation of any federal, state, or local law.
 - sending, receiving, viewing or downloading illegal material via the computer system.
 - unauthorized downloading of software.
 - using the computer system for private financial or commercial purposes.
 - wastefully using resources, such as file space.
 - gaining unauthorized access to resources or entities.
 - posting material created by another without his or her consent.
 - submitting, posting, publishing, or displaying any obscene, profane, threatening, illegal, or other inappropriate material.
 - using the computer system while access privileges are suspended or revoked.
 - vandalizing the computer system, including destroying data by creating or spreading viruses or by other means.
 - intimidating, harassing, bullying, or coercing others.
 - threatening illegal or immoral acts.

4. **Network Etiquette.** Each user is expected to abide by generally accepted rules of etiquette, including the following:
 - be polite.
 - users shall not forge, intercept or interfere with electronic mail messages.
 - use appropriate language. The use of obscene, lewd, profane, lascivious, threatening or disrespectful language is prohibited.
 - users shall not post personal information other than directory information as defined in Policy JO Student Records about themselves or others.
 - users shall respect the computer system's resource limits.
 - users shall not post chain letters or download large files.
 - users shall not use the computer system to disrupt others.
 - users shall not modify or delete data owned by others.

5. **Liability.** The School Board makes no warranties for the computer system it provides. The School Board 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 School Division denies any responsibility for the accuracy or quality of information obtained through the computer system. The user agrees to indemnify the School Board for any losses, costs, or damages incurred by the School Board relating to or arising out of any violation of these procedures.

6. **Security.** Computer system security is a high priority for the school division. If any user identifies a security problem, the user shall notify the building principal or system administrator immediately. All users shall keep their passwords confidential and shall follow computer virus protection procedures.

7. **Vandalism.** Intentional destruction of or interference with any part of the computer system through creating or downloading computer viruses or by any other means is prohibited.

8. **Charges.** The School Division assumes no responsibility for any unauthorized charges or fees as a result of using the computer system, including telephone, data, or long-distance charges.

9. **Electronic Mail.** The School Division's electronic mail system is owned and controlled by the School Division. The School Division may provide electronic mail to aid students and staff in fulfilling their duties and as an education tool. Electronic mail is not private. Students' electronic mail will be monitored. The electronic mail of staff may be monitored and accessed by the School Division. All electronic mail may be archived. Unauthorized access to an electronic mail account by any student or employee is prohibited. Users may be held responsible and personally liable for the content of any electronic message they create or that is created under their account or password. Downloading any file attached to an electronic message is prohibited unless the user is certain of that message's authenticity and the nature of the file.

10. **Social Media.** "Social Media" refers to forms of electronic communication, such as Web sites for social networking and microblogging, through which users create online communities to share information, ideas, personal messages, and other content, such as videos. Social media includes, but is not limited to, sites such as Facebook, Twitter, and MySpace.

The use of social media on the School Division's computer network is addressed in regulation GAB-R / IBEA-R. This policy addresses employees' use of social media on personal devices.

School Division employees are prohibited from using personal devices to post to social media for personal reasons during work hours.

When using social media outside of work hours, School Division employees should be aware that such use or postings, even if personal or seemingly private, may be viewed by students, parents, colleagues and others and that offensive or inappropriate content could result in professional repercussions.

School Division employees should also be aware that personal communications with students via social media may be construed as inappropriate. It is recommended that School Division employees refrain from engaging in personal communications with students via social media or personal e-mail accounts.

The School Division's computer system shall not be used to access, post to, view, or otherwise use social media, which includes, but is not limited to Facebook, Twitter, and MySpace, for personal reasons, unless such use is consistent with Policy IBEA/GAB and this regulation and is approved in advance. School Division employees must get approval from their immediate supervisor or building principal and student Users must get approval from their teacher before using social media on the School Division's computer system.

When any User has been given approval to use the School Division's network for social media, the User must:

- a. Identify himself and his position truthfully;
- b. Conduct himself in a professional manner;
- c. Refrain from posting confidential information regarding any student, parent, or Division employee;
- d. Use correct spelling and grammar; and
- e. Conduct himself in a manner consistent with School Board policy, including but not limited to, the policies prohibiting discrimination and harassment, Policies GB and GBA.

11. **Enforcement.** Software will be installed on the division's computers having Internet access to filter or block internet access through such computers to child pornography and obscenity. The online activities of users may also be monitored manually. **Any violation of these regulations shall result in loss of computer system privileges and may also result in appropriate disciplinary action, as determined by School Board policy, or legal action.**

Adopted: June 10, 2013
 Adopted: August 19, 2013
 Amended: August 18, 2014

Legal Refs: 18 U.S.C. §§ 1460, 2256.
 47 U.S.C. § 254.

Code of Virginia, 1950, as amended, §§ 18.2-372, 18.2-374.1:1, 18.2-390, 22.1-70.2 and 22.1-78.

Guidelines and Resources for Internet Safety in Schools, Virginia Department of Education (Second Edition October 2007)

Cross Refs: GCPD Professional Staff Discipline
 JFC Student Conduct
 JFC-R Standards of Student Conduct