ACCEPTABLE COMPUTER SYSTEM USE

All use of the Patrick 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.
   - accessing or attempt to access another person's account or files without prior consent of that person.
   - downloading, uploading, or distributing any files, software, or other material in violation of fair-use and copyright laws of intellectual property laws.
   - 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.
   - gaining unauthorized access to resources or entities.
   - posting material created by another without his or her consent.
   - accessing, 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.

   Filter with Regard to Internet Access: Only division-provided Internet access should be used for utilizing the Internet within the division. At no time may any electronic or mechanical device be used with an unfiltered connection to the Internet or to intimidate, antagonize, or otherwise harm other students, teachers, administrators, or visitors.

   Students should never give out personal information without an adult's permission, especially if it conveys where they are located at a particular time.

   Students and their families should discuss how to identify acceptable sites to visit and what to do if an inappropriate site is accessed. Students should be informed about various web advertising techniques and realize that not all sites provide truthful information.

   Students and their families should discuss acceptable social networking and communication methods and the appropriate steps to take when encountering a problem. Students should know the potential dangers of emailing, gaming, downloading files, and peer-to-peer computing (e.g., viruses, legal issues, harassment, sexual predators, identity theft).

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. **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: April 7, 2005
Revised: July 16, 2009
July 11, 2013
March 8, 2018

_____

_____