

ACCEPTABLE USE POLICY (AUP) & INTERNET SAFETY

Mathews County School Division's computer systems use shall be consistent with the goal of promoting educational excellence by facilitating resource sharing, innovation and communication. The term computer system includes, computer equipment; software; operating systems; storage media; network accounts providing access to network services, such as email; Web browsing and file systems; security systems including key pads and monitors; as well as telecommunication technologies such as telephones, personal computers, cellular phones, Personal Digital Assistants (PDAs), facsimile machines, and all other wired or wireless telecommunication devices. This policy shall apply to all current and emerging information and telecommunication technologies.

Computer System Use-Terms and Conditions:

1. **Privacy.** Employees and students have no expectation of privacy in their use of school computers, Internet services or computer systems. The use of the computer systems or related services is not intended to create an open or limited forum under the First Amendment to the Federal or State constitutions. The Division retains the right to monitor all computer, computer systems and Internet activity by employees, students and other users. Any information or communications on the computer systems and network services may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Use of the Division's computers, networks, and Internet systems is a privilege, not a right, and can be withdrawn by the Division at any time.
2. **Acceptable Use.** Access to the Division's computer systems 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.
 - Incidental personal use is limited to times outside of instructional or duty time and must not impact use of the computer systems by other users or be in violation of the AUP, school, department, or other division policies and regulations.
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.
 - Any use for a forum for communicating by email or any other medium with other school users or outside parties to solicit, proselytize, advocate, or communicate the views of an individual or non-school-sponsored organization; to solicit membership in or support of any non-school sponsored organization; or to raise funds for any non-school sponsored

purpose, whether profit or non-profit. Employees who are uncertain as to whether particular activities are acceptable shall seek further guidance from their supervisor, Division Superintendent or designee.

- Knowingly provide email addresses to outside parties whose intent is to communicate with school employees, students and/or their families for non-school purposes. Employees who are uncertain as to whether particular activities are acceptable shall seek further guidance from their supervisor, Division Superintendent or designee.
- Leaving any computer system or device accessible to unauthorized users.
- Leaving passwords or other access devices and keys in an unsecure location or writing down passwords and storing them anywhere accessible to others as well as storing passwords in a file on ANY computer system (including PDAs or similar devices) without encryption.
- Copying, providing, receiving or using another users' log-on information, building security electronic key and pin number, or any user specific password, electronic access or key device issued by the Division.
- Use of administrative, faculty and staff computer access or other administrative computer systems access by, students, guests, visitors and family members.
- Sending, receiving, viewing, uploading or downloading illegal material via the computer system.
- Unauthorized downloading or uploading of software, music/videos and other forms of copyrighted material.
- Using the computer system for private financial or commercial purposes.
- Wastefully using resources, such as file space, Internet bandwidth, wide area network bandwidth and computer or computer systems access.
- Sending mass emails to school users or outside parties for school or non-school purposes without the permission of an administrator.
- Any attempt to delete, erase or otherwise conceal any information stored on computer systems which violates AUP rules, State, Federal or Local law or at any time after being advised by any administrator or supervisor to preserve any materials stored on a computer or computer system.

- Attempting or gaining unauthorized access to computer systems, entities, resources including but not limited to any computer device, network file, folder, data and information.
 - Copying, emailing, forwarding, posting, printing or uploading any content or email created by another without his or her consent.
 - Submitting, posting, publishing or displaying any obscene, profane, threatening, illegal or other inappropriate material.
 - Cyber bullying, threatening, or using the computer system to disrupt the school learning environment.
 - Using the computer system while access privileges are suspended or revoked.
 - Vandalizing or interfering with any part of the computer systems, including physical and electronic damage, destroying data by creating, emailing or using any other method to spread, adware, malware, viruses, and spyware.
 - Intimidating, harassing, 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. Use of computers and other electronic devices in a manner that disrupts the learning environment, activities or events is prohibited.
 - Users shall not forge, intercept or interfere with electronic transmissions.
 - 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 unless they have received written permission from that person or the posting and printing meets all district and school policies and regulations.
 - Users shall respect the computer system's resource limits.
 - Users shall not forward or post chain letters or similar types of emails.
 - Users shall not modify or delete data or printed material owned by others without their permission.

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, key pad pin codes and network access codes and keys confidential and shall follow computer malware, spyware and virus protection procedures. Users are responsible for maintaining vigilance over all district computer systems they use and following AUP and other associated policies and procedures even if using remote access or a non-district supplied device to connect to the district's computer system.
7. **Internet Filtering.** As required by the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)], Internet blocking and filtering shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized for a bona fide research or other lawful purposes. It shall be the responsibility of all Mathews County Public staff to supervise and monitor usage of the computer network and access to the Internet in accordance with applicable Federal and State laws, guidelines, and regulations of the Virginia Department of Education, and School Board policies and regulations.
8. **Charges.** The School Division assumes no responsibility for any unauthorized charges or fees as a result of using the computer system, including credit card, debit card, account charges and telephone or long-distance charges.
9. **Electronic Mail.** The School Division's electronic mail system is owned and controlled by the School Division and may be monitored and accessed by the School Division. Unauthorized access to an electronic mail account by any student or employee is prohibited. Users shall be held personally liable for the content of any electronic message they create. 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. **Instructional Philosophies Related to the Acceptable Use and Internet Safety Policy.** Each school will provide students' integrated ongoing Internet safety instruction at all grade levels and subject areas. The school division will provide parents, guardians and community organizations that serve division students, selected materials and resources to facilitate Internet safety awareness, training, skill attainment and application of knowledge already learned. Mathews County Public Schools will guide student use of computer systems through the Acceptable Computer Use Policy (AUP) and other school and classroom specific policies, procedures and regulations. These policies will be provided to students and their parents or guardians each school year. Internet safety will be an integrated feature embedded in student instruction throughout the school year.

11. **Strategies Related to the Acceptable Use and Internet Safety Policy.** Ultimately, it is the individual computer system user that is responsible for their actions and what they access while using computer systems. Division schools use Federal and State compliant Internet filtering, security and email software on all computer systems in addition to updated virus, intrusion and spy-ware protection. Although these technological systems are intended to protect students and division data and information, no system is 100% effective. Monitoring and observation using non-technical means is just as important to Internet safety and data security and is the responsibility of all division employees.

All student and guest access computers screens are to be placed so that the employee supervising these computers can visually or electronically monitor activities. All office and staff computers screens are to be placed away from student and public view. When administrative, teacher or staff computers are left unattended they should be locked and the screen blanked out to prevent unauthorized access or viewing.

12. **Internet Safety and Security Instruction.** The Division will maintain an Internet Safety Resource Web page that includes current and diverse resources that can be used by the school board, administrators (central office and building), teachers, teacher assistants, counselors, instructional technology resource teachers, library media specialists, building resource officers, technology coordinator, students and community stakeholders. (Including but not limited to parents, caregivers, public library staff, after-school and off-campus program instructors and local law enforcement officials.) Online distance learning opportunities are available to division Administrators, Faculty, Staff and Students through the division's course management system.

13.

Internet safety and security instruction is the responsibility of all instructional personnel at all grade levels and subject areas. The division uses the I-Safe and NetSmartz curriculum which is structured by grade level or student age. The division will maintain or have access to certified instructors that can deliver Internet safety staff development instruction to all staff members on an annual ongoing basis. School level anti-bullying programs as well as relationships already established with local law enforcement programs through the School Resource Officers will include Internet safety components.

Mathews County Schools recognizes that computer system use is not limited to the school environment and as such Internet Safety and Security awareness and vigilance must be provided for school and after school use of computer systems.

The division will regularly organize, participate and promote Internet safety through PTA meetings, newsletters, consortium and grant related materials and training, public television and radio programs, 4-H events, scout meetings, Rotary and other community organization events and meetings. Free Internet safety materials and media will be available in public spaces such as the school libraries and be given to students, parents and guardians on request.

13. **Review Process.** The Division Technology Steering Committee and each school level technology committee are responsible for reviewing the AUP policy, regulation and Internet safety program annually. Each building administrator will add Internet safety to their lesson plan and evaluation review of instructional personnel. Every two years, the Division Superintendent will file an updated Acceptable Use Policy with the State that has been approved by the Mathews County School Board.
14. **Enforcement.** Hardware and software is installed on the School Division's computer systems to monitor various activities that include but are not limited to filtering or blocking access to child pornography, obscenity and other activities as outlined in the Children's Internet Protection Act (CIPA) in addition to other Federal, State and Local policies and regulations. Manual monitoring of students, staff and other users of the division's computer systems by employees designated by the superintendent may be used to supplement automated monitoring. **Any violation of these regulations shall result in loss of computer system privileges and may also result in appropriate disciplinary action, as determined by Mathews County School Board policy, school policy, administrative policy or legal action.**

Adopted: July 19, 2005
Amended: April 11, 2006
Amended: August 19, 2008
Adopted: July 21, 2009

Legal Refs: 18 U.S.C. §§ 1460, 2256.
47 U.S.C. § 254, Pub. Law 106-554 § 1 (a) (4), 20 U.S.C. § 1232g, et seq.;
34 CFR 99, 20 U.S.C. § 1232h, and 34 CFR 98.
Code of Virginia, 1950, as amended, § 18.2-372, 18.2-374.1:1, 18.2-390,
22.1-70.2, 212.2:3, 22.1-78, and “Guidelines and Resources for Internet
Safety in Schools,” Virginia Department of Education, October 2007.

Cross Refs:

GCPD	Professional Staff Members: Contract Status and Discipline
GDPD	Support Staff Members: Contract Status and Discipline
JFC	Student Conduct
JFC-R	Standards of Student Conduct