

## ACCEPTABLE COMPUTER SYSTEM USE

All use of the **Mecklenburg 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, display devices, printers, CD, DVD and other media devices, tape or flash drives, storage devices, servers, mainframe and personal computers, tablets, laptops, telephones, cameras, projectors, multimedia devices, workstations, the internet and other electronic services and any other internal or external network. This includes any device that may be connected to or used to connect to the school division's network or electronically stored division material.

### **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. **General Use and Ownership.**
  - Mecklenburg County Public Schools proprietary information stored on electronic and computing devices whether owned or leased by Mecklenburg County Public Schools, the employee or a third party, remains the sole property of Mecklenburg County Public Schools.
  - You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Mecklenburg County Public Schools proprietary information.
  - You may access, use or share Mecklenburg County Public Schools proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
  - Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
  - For security and network maintenance purposes, authorized individuals within Mecklenburg County Public Schools may monitor equipment, systems and network traffic at any time.
  - Mecklenburg County Public Schools reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
3. **Security and Proprietary Information.**
  - System level and user level passwords must have complexity (employee and secondary students). Complexity is the use of uppercase and lowercase lettering, numbers and symbols. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
  - All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 30 minutes or less. You must lock the screen or log off when the device is unattended.

4. **Privilege.** The use of the division's computer system is a privilege, not a right.
  
5. **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.
  - Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee/student is not an intended recipient or logging into a server or account that the the employee/student is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
  - Port scanning or security scanning is expressly prohibited unless prior notification to Technology Department is made.
  - Executing any form of network monitoring which will intercept data not intended for the divisions host, unless this activity is a part of the employee's normal job/duty.
  - Circumventing user authentication or security of any host, network or account.
  - Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
  - Providing information about, or lists of, Mecklenburg County Public Schools employees/students to parties outside Mecklenburg County Public Schools.
  - Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. **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.
  
7. **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 is not responsible 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.
  
8. **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.
  
9. **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.
  
10. **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.
  
11. **Student Supervisory Guidelines.** Teachers will provide students with a sequential, structured approach to gaining the skills that will allow them to become independent, responsible users of the computer network or Internet. In all classes, teachers will make a reasonable effort to ensure that students are directed to sites with age and topic appropriate materials and resources.
  - In K-3, teachers will actively supervise student use of the computer network and Internet. Students will only access Internet resources previously explored by the teacher.

- In grades 4-5, teachers will supervise and model appropriate use of the computer network and Internet. Students will continue to have computer network and Internet access under direct teacher supervision. However, students will experience guided practice leading toward gaining skills to become independent and responsible users of the Internet. Teachers will explore an Internet site before directing students to that site.
  - In grades 6-8, teachers will provide guided practice and model appropriate use of the computer network and Internet. Teachers will supervise student-initiated information-search activities and provide support for students as they begin to assume responsibility for becoming independent users of the computer network and Internet.
  - In grades 9-12, students will participate in independent computer network and Internet use with teachers serving as advisors and providing monitoring as appropriate.
12. **Photographs, Artwork, Videos, and Audio Materials.** Photographs, artwork, videos and audio materials will be presented in such a way to protect the individual student. These materials may be used in newspapers, television, or the Mecklenburg County Public Schools website and social media pages only if the parent /guardian has signed and returned the Mecklenburg County Public Schools Acceptable Use Policy.
13. **Blogging/Social Media.**
- Blogging by employees and/or students, whether using Mecklenburg County Public Schools' property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Mecklenburg County Public Schools' systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Mecklenburg County Public Schools' policy, is not detrimental to Mecklenburg County Public Schools' best interests, and does not interfere with an employee's regular work duties. Blogging from Mecklenburg County Public Schools' systems is also subject to monitoring.
  - Employees and/or students shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Mecklenburg County Public Schools and/or any of its employees and/or students. Employees and/or students are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Mecklenburg County Public Schools' *Non-Discrimination and Anti-Harassment* policy.
  - Employees and/or students may also not attribute personal statements, opinions or beliefs to Mecklenburg County Public Schools when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee and/or student or representative of

Mecklenburg County Public Schools. Employees and/or students assume any and all risk associated with blogging.

- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Mecklenburg County Public Schools' trademarks, logos and any other Mecklenburg County Public Schools intellectual property may also not be used in connection with any blogging activity

14. **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.
15. **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: July 29, 2019

---

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

## ACCEPTABLE COMPUTER SYSTEM USE

The School Board provides a computer system, including the internet, to promote educational excellence by facilitating learning, resource sharing, innovation and communication. The term computer system includes, but is not limited to, hardware, software, data, communication lines and devices, terminals, display devices, printers, CD, DVD and other media devices, tape or flash drives, storage devices, servers, mainframe and personal computers, tablets, laptops, telephones, cameras, projectors, interactive whiteboards/panels, audio-visual equipment, multimedia devices, workstations, remote network access, cloud services, the internet and other electronic services and internal or external networks. This includes any device that may be connected to or used to connect to the school division's network or electronically stored division material.

All use of the division's computer system must be (1) in support of education and/or research, or (2) for legitimate division business. Use of the computer system is a privilege, not a right. Inappropriate use may result in cancellation of those privileges, disciplinary action, and/or legal action. Any communication or material generated using the computer system, including electronic mail, social media posts, instant or text messages, tweets, and other files, including communications and materials deleted from a user's account, may be monitored, read, and/or archived by division staff.

This policy applies to all users of the division's computer system. By using or accessing the computer system, the user agrees to abide by this policy and the Technology Use Guidelines established by the superintendent.

The superintendent is responsible for establishing Technology Use Guidelines, containing the appropriate uses, ethics and protocols for use of the computer system. The superintendent is also responsible for reviewing and updating, as necessary, the Guidelines at least every two years. It is the user's responsibility to know and follow this policy and the Technology Use Guidelines.

The Guidelines include:

- (1) a prohibition against use of the division's computer equipment and communications services for sending, receiving, viewing or downloading illegal material via the internet;
- (2) provisions, including the selection and operation of a technology protection measure for the division's computers having internet access to filter or block internet access through such computers, that seek to prevent 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;

- (3) provisions establishing that the technology protection measure is enforced during any use of the division's computers;
- (4) provisions establishing that all usage of the computer system may be monitored;
- (5) provisions designed to educate students and employees about appropriate online behavior, including interacting with students and other individuals on social networking websites, blogs, in chat rooms, and cyberbullying awareness and response;
- (6) provisions designed to prevent unauthorized online access by minors, including "hacking" and other unlawful online activities;
- (7) provisions requiring every user to protect the security of information necessary to access the computer system, such as usernames and passwords, and prohibiting the sharing of passwords;
- (8) provisions prohibiting the unauthorized disclosure, use, and dissemination of photographs and/or personal information of or regarding minors; and
- (9) a component of internet safety for students that is integrated in the division's instructional program.

Use of the school division's computer system must be consistent with the educational or instructional mission or administrative function of the division as well as the varied instructional needs, learning styles, abilities and developmental levels of students.

The division's computer system is not a public forum.

Users of the division's computer system have no expectation of privacy for use of the division's resources or electronic devices including non-division owned devices while connected to division networks or computer resources.

Software and/or services may not be installed or downloaded on the division's computer system without the prior approval of the superintendent or superintendent's designee.

No employee or agent of the School Board or person or entity contracting with the School Board may download or use any application, including TikTok or WeChat, or access any website developed by ByteDance Ltd. or Tencent Holdings Ltd. (i) on any device or equipment issued, owned, or leased by the School Board, including mobile phones, desktop computers, laptop computers, tablets, or other devices capable of connecting to the Internet.

The failure of any user to follow the terms of this policy or the Technology Use Guidelines may result in loss of computer system privileges, disciplinary action, and/or appropriate legal action. Users of the system agree to indemnify the School Board for any losses, costs, or damages relating to or arising out of any violation of this policy or the Technology Use Guidelines.

The School Board is not responsible for any information that may be lost, damaged or unavailable when using the computer system or for any information retrieved via the internet. Furthermore, the School Board is not responsible for any unauthorized charges or fees resulting from access to the computer system.

The School Board reviews and amends, if necessary, this policy every two years.

Adopted: December 15, 2014

Revised: July 29, 2019; July 19, 2021; July 31, 2023

---

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

Code of Virginia, 1950, as amended, §§ 2.2-5514.1, 18.2-372, 18.2-374.1:1, 18.2-390, 22.1-23.3, 22.1-70.2, and 22.1-78.

Cross Refs.: ECAB                      Vandalism  
EGAA                                  Reproduction and Use of Copyrighted Materials  
GBA/JHFA                              Prohibition Against Harassment and Retaliation  
GCPD                                    Professional Staff Discipline  
GCQB                                    Staff Research and Publishing  
JFC                                        Student Conduct





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 every year 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 \_\_\_\_\_

Student/Employee Name \_\_\_\_\_ (Please Print)

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 **Mecklenburg 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 Mecklenburg County School Division's policies and regulations and for the School Division to issue an account for my student.

- I grant permission for photographs, artwork, videos and audio materials of my child to be used in the newspapers, television or the division's websites.
- I **DO NOT** grant permission for photographs, artwork, videos and audio materials of my child to be used in the newspapers, television or the division's websites.

Parent/Guardian Signature \_\_\_\_\_ Date \_\_\_\_\_

Parent/Guardian Name \_\_\_\_\_ (Please Print)