

BOARD OF EDUCATION
POLICY 8080
ACCEPTABLE USE OF COMPUTER
TECHNOLOGY

Effective: July 1, 2007

I. Policy Statement

The Board of Education of Howard County recognizes that as new computer technologies change the ways that information may be accessed, communicated, and transferred, those changes also provide new opportunities and responsibilities for students and employees. Learning how to use computer technologies is fundamental to preparing students as citizens. The Board expects that employees will integrate thoughtful use of computer technologies throughout the curriculum and instruction, and will apply them appropriately in the performance of tasks associated with their responsibilities and positions. The Board also recognizes that school system hardware, software, and information stored using computer technologies must be protected from unauthorized access, modification, destruction, or distribution, whether accidental or intentional.

The Board is committed to providing appropriate access by employees and students to computer technology in furtherance of the educational goals and objectives of the school system. The Board recognizes the consequent need to take reasonable precautions against misconduct by establishing guidelines for acceptable use of computer technology. In exchange for access to the school system's computer technology, users are expected to employ these resources in a responsible, ethical, and legal manner. The misuse of the school system's computer technology is grounds for discipline and/or denial of access.

II. Purpose

The purpose of this policy is to provide direction related to maintaining the integrity of school system computer technology and the security of electronic information as well as utilizing computer technology to the maximum extent possible consistent with appropriate use.

III. Definitions

- A. Computer Technology – For purposes of this policy, all hardware and software, including files, records, e-mail, and other data.
- B. E-mail – A means or system for transmitting messages electronically (as between computers on a network); messages sent and received electronically through such means or system.

- C. Hardware – The mechanical, magnetic, electronic design, structure, and devices of a computer. Hardware includes but is not limited to personal computers, servers, networks, terminals, laptops, portable devices, and related peripherals. These devices may have hardwire and/or wireless connections.
- D. Internet – A "network of networked computers" that consists of millions of smaller domestic, academic, business, and government networks, which together carry various information and services, such as electronic mail, online chat, file transfer, and the interlinked Web pages and other documents of the World Wide Web.
- E. Software – The programs, data, routines, and operating information used in a computer or on a network; includes access to the World Wide Web (Internet).
- F. System Administrator – The Superintendent's designee responsible for implementing and maintaining the school system's hardware and software infrastructure; enforcing related policies, including internal and external access and security; and managing service technicians.

IV. Standards

- A. Access to school system computer technology will be provided only in accordance with the procedures associated with this policy.
- B. Electronic communications transmitted using the school system's computer technology (e.g. e-mail, teacher websites, podcasts, webcasts, blogs, etc.) or school system's portable communications devices (e.g., cellular phones, wireless devices) are subject to the Student Code of Conduct; Policy 1040, Safe School Environments; and Policy 7030, Employee Discipline.
- C. School system computer technology is intended for instructional use and school-related business. It is not intended for personal, commercial, profitable, religious, or political use, except as such uses are permissible and authorized under Policy 10020, Use of School Facilities by Non-School Groups.
- D. School system computer technology is available for infrequent personal use so long as the use does not interfere with student or employee work, cause disruptions to the school or work environment, or violate school system policies or applicable laws.
- E. The school system will not guarantee the availability of access to the Internet or school system computer technology and will not be responsible for any information that may be lost, damaged, or unavailable due to technical or other difficulties.

- F. Access to school system computer technology granted by virtue of the user's status as an employee, student, volunteer, or contracted employee or for a specific purpose will be terminated when the relationship is terminated or the purpose is fulfilled.
- G. All software used for instructional purposes must be approved in accordance with Policy 8040, Selection of Instructional Materials and must be in compliance with licensing and/or fair use agreements. Software used by employees for administrative productivity must be in compliance with licensing and/or fair use agreements.
- H. The school system reserves the right to restrict access to certain electronic information.
- I. Student records which are maintained electronically must be maintained in a confidential and secure manner in accordance with Policy 9050, Student Records and Confidentiality.
- J. The school system reserves the right to purge files stored in user's individual technology accounts.
- K. The school system has the right to access, archive, and disclose the contents of electronic communications, files, and other material created, stored, or accessed using school system computer technologies as required by the system's legal, audit, and legitimate operational purposes. Access must be authorized by the Superintendent/designee. If the review shows violation of this policy, appropriate actions may be taken. Users should have no privacy expectations in the contents of their individual electronic files and records of their online activity while using the school system computer technology.
- L. The school system retains the right to editorial oversight of central office, departmental, or school electronic publications such as websites and newsletters.
- M. The school system is committed to the implementation of the Children's Internet Protection Act (CIPA). In order to comply with CIPA, computer technology which attempts to filter abusive, libelous, obscene, offensive, profane, threatening, sexually explicit, pornographic, or illegal material will be employed.
- N. Reassignment of hardware between schools, offices, or other physical locations requires the approval of the System Administrator and compliance, when applicable, with Policy 4040, Fixed Assets.
- O. The school system will periodically establish standards for hardware and software. These standards will establish what hardware and software may be used

on the school system network and what technical support may be provided by the school system.

- P. Unauthorized costs incurred by users of school system computer technology shall be the responsibility of the user incurring the cost.
- Q. Notice of the provisions of this policy and user responsibilities shall be communicated to all students, parents, employees, and users of the school system's computer technology.
- R. Failure by any user to comply with this policy may result in the temporary or permanent termination of computer access privileges.
- S. Violations of this policy by an employee may result in disciplinary action such as a letter of warning, a letter of reprimand, suspension without pay, or dismissal by the Superintendent.
- T. Violations of this policy by a student may result in disciplinary action under the guidelines of Policy 9200, Discipline and the Student Code of Conduct.
- U. Individuals or organizations using school system computer technology as part of an agreement to use school system facilities (including those who are using the facilities in accordance with Policy 10020, Use of School Facilities by Non-School Groups) are subject to the provisions of this policy.

V. Compliance

- A. The Superintendent's designee will establish guidelines and appropriate forms for the use of computer technology.
- B. Principals are responsible for notifying students, families, volunteers and employees in their schools of the provisions of this policy.
- C. The Superintendent's designee is responsible for communicating the provisions of this policy annually through customary channels.
- D. The Principal/designee or Building Manager is responsible for notifying individuals or organizations seeking to use school system computer technology as part of an agreement to use school system facilities under Policy 10020, Use of School Facilities by Non-School Groups, of the provisions of this policy.
- E. The System Administrator/designee must approve software before installation.

- F. The Superintendent's designee is responsible for reviewing this policy at least every three years and recommending it for revision as necessary.
- G. The System Administrator is responsible for establishing prudent measures to safeguard the security of school system computer technology and electronic information.

VI. Delegation of Authority

The Superintendent is authorized to develop procedures for the implementation of this policy.

VII. References

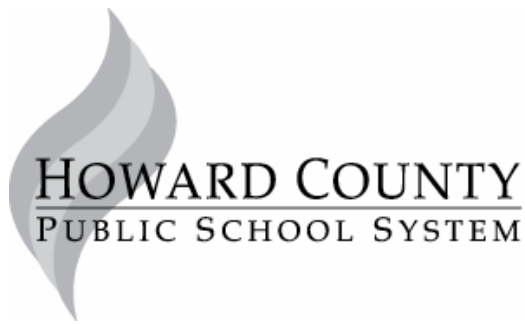
- A. Legal
 - Electronic Communications Privacy Act, 18 U.S.C. §2701-2711
 - Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232(g)
 - Section 508 of the Rehabilitation Act of 1973, 20 U.S.C. §794(d)
 - Title VII of the Civil Rights Act of 1964, 42 U.S.C. §2000(e)
 - Title XVII, Children's Internet Protection Act, as codified at 47 U.S.C. §254(h)
- B. Other Board Policies
 - Policy 1000 Civility
 - Policy 1040 Safe School Environments
 - Policy 4040 Fixed Assets
 - Policy 7030 Employee Discipline
 - Policy 8040 Selection of Instructional Materials
 - Policy 8120 Testing: State and Local Responsibilities and Protocols
 - Policy 9030 Student Publications and Productions
 - Policy 9050 Student Records and Confidentiality
 - Policy 9200 Discipline
 - Policy 10010 Distribution and Display of Materials and Announcements
 - Policy 10020 Use of School Facilities by Non-School Groups
- C. Other
 - Ethics Regulations
 - Student Code of Conduct

ADOPTED: November 26, 2002

AMENDED: January 21, 2003

May 10, 2007

EFFECTIVE: July 1, 2007



POLICY 8080-PR
IMPLEMENTATION PROCEDURES
**ACCEPTABLE USE OF COMPUTER
TECHNOLOGY**

Effective: July 1, 2007

I. Announcement/Dissemination of Information

- A. Notification of the provisions of Policy 8080 and these procedures should be given on a regular basis to all students, families, employees, and service providers. Notification may be:
1. Announced in schools over the public address system at the beginning of the school year and at other times deemed appropriate
 2. Published in school and system newsletters and/or handbooks
 3. Posted in areas that provide access to computer technology (e.g., media center, computer lab)
 4. Posted on school and system websites
 5. Reviewed with students by classroom teachers, media specialists, or other appropriate employees
 6. Incorporated, whenever possible and appropriate, into the process of accessing software and/or files.
- B. Principals are responsible for notifying all students, families, volunteers, and employees in their schools of the responsibilities of users of school system computer technology and of guidelines for network activities at the beginning of the school year, with reminders throughout the year.
- C. Supervisors are responsible for notifying those under their supervision of the provisions of Policy 8080 and these procedures.
- D. The Building Manager is responsible for notifying individuals or organizations seeking to use school system computer technology as part of an agreement to use school system facilities under Policy 10020, Use of School Facilities by Non-School Groups, of the provisions of Policy 8080 and these procedures.

II. User Responsibilities

- A. The following are applicable to all users of the school system's computer technology:
1. Users are responsible for taking reasonable precautions to protect school system owned technology equipment against damage and/or theft.
 2. Users are responsible for using school/school system-provided technology accounts (whether onsite or remotely) in an ethical, efficient, responsible, and legal manner.
 3. Users shall not reveal personally identifiable information about others to any third party unless required to do so by their professional responsibilities. Disclosure of student information is addressed in Policy 9050, Student Records and Confidentiality.
 4. Users will employ resources on computer technology in accordance with the policies of the institutions providing the service, as well as the procedures developed by the school system.
 5. Users will not engage in unauthorized activities. These include, but are not limited to:
 - a. Accessing unauthorized information
 - b. Accessing information prohibited by the provisions of Policy 8080 and these procedures
 - c. Knowingly spreading computer viruses
 - d. Violating copyright laws or the privacy rights of others
 - e. Plagiarism
 - f. Accessing computer technology network via another user's account or facilitating unauthorized access by another
 - g. Entering (hacking) into, destroying (including physical destruction) school system computer technology and files, or disrupting the network
 - h. Circumventing/disabling filtering or other computer technology protection measures put in place by the System Administrator, without proper authorization
 - i. Using software or hardware on the school system network which is not in compliance with current standards
 6. Users are encouraged to remove outdated files from individual account spaces. Outdated files may be purged from time to time. Reasonable effort will be made to notify account holders prior to routine purging of stored messages.

7. Users are responsible for files stored on school system computers, servers, and digital media.
- B. The following apply to the use of computer technology by employees:
1. Employees are to use school system computer technology in a responsible, ethical manner consistent with their professional responsibilities.
 2. Employees will not create, access, download, store, or print files, messages, or images that are violent, defamatory, vulgar or sexually explicit, or that would otherwise cause a disruption to the school environment, unless required by their professional responsibilities.
 3. For the protection of all parties, when using e-mail to correspond with parents and students, employees must use the school system's e-mail system. Employees are responsible for all e-mail sent from their accounts.
 4. Employees must ensure that they comply with the confidentiality requirements of Policy 9050, Student Records and Confidentiality, when creating backup copies of student records or transmitting confidential student records electronically.
 5. If employees install software on school system computers that conflicts with the standard school system disk image, the system reserves the right to re-image the computers.
 6. Employees responsible for central office, departmental, or school electronic publications such as websites and newsletters will ensure that:
 - a. The Principal/central office or department supervisor approves the content of publications
 - b. Only authorized employees post files to the school system server
 - c. Written permission is obtained and kept on file for any copyrighted material or student work used in publications
 - d. Students are not identified by name in photographs used in publications unless written permission from their parents is obtained and kept on file
 - e. Commercial links and/or advertising are minimized, must be monitored for appropriateness, and where applicable must comply with Policy 4010, Donations
 - f. Student publications are subject to Policy 9030, Student Publications and Productions.

7. Employees assigning directed Internet use by students will prescreen network resources in order to specify those which are applicable to the curricular needs of the assignment and the developmental level of the student(s). Employees are responsible for providing appropriate adult supervision and monitoring of learning activities.
8. Independent Internet activities are permitted at the high school level only. Employees assigning independent Internet activities will ensure that such activities and available resources are applicable to the curricular needs of the assignments and the developmental levels of the students, and that signed school system permission forms for student independent access are on file for all students participating in the activities. Each high school must provide for the distribution, collection, and maintenance of the permission forms. See section II.C.7.
9. Employees assigning or permitting use of computer technology by students will ensure that instruction in acceptable use of computer technology has occurred. Topics to be taught include:
 - a. The contents of Policy 8080 and these procedures
 - b. Procedures for accessing appropriate network resources
 - c. Procedures for using specific Internet tools
 - d. Provisions contained in school system Internet permission forms (high school students only)
 - e. Copyright issues
 - f. Privacy issues
 - g. Safety guidelines on the Internet
 - h. Respect for time and resource use
 - i. Acquiring skills needed to make judgments about locating and using information, which matches the learner's instructional level and the learning objectives of the assignment
 - j. Discriminating among types of information sources and assessing the appropriateness of using the Internet as a resource for a specific learning activity
 - k. Applying the same criticism of educational accuracy and suitability used for all educational resources.
10. Software that is developed within the school system curriculum may be installed and used at the discretion of the instructor.
11. When sending confidential material electronically the recipients should be alerted to the confidential nature of the message in accordance with FERPA (Family Educational Rights and Privacy Act). Whenever possible the use of student identifiers should be avoided in e-mail.

12. Online gradebook software must be approved through the software approval process, in accordance with Policy 8040, Selection of Instructional Materials.
 13. Web tools and sites which support collaborative discussions (i.e. Wikis, blogs, instant messaging, threaded discussions, social networking sites) must be approved through the software approval process prior to use for instruction and associated student generated work must be monitored for appropriateness. Students must adhere to Policy 1000, Civility; the Student Code of Conduct; and Policy 1040, Safe School Environments when accessing and posting to these tools and sites.
- C. The following apply to student use of school system computer technology:
1. Students are responsible for their behavior on school computer networks.
 2. Students may not reveal personally identifiable information (e.g., home phone numbers, addresses, or social security numbers) except in specific circumstances where such information is required to complete academic assignments; in such circumstances prior written consent from the parent of the student whose information is being posted or transmitted is required.
 3. Students will access only those network resources for which they have obtained permission, using only the account assigned to them.
 4. Students will not create, access, download, store, or print files, messages or images that:
 - a. Depict profanity, obscenity, the use of weapons, or violence
 - b. Promote use of tobacco, drugs, alcohol, or other illegal or harmful products
 - c. Contain sexually suggestive messages
 - d. Are sexually explicit or obscene
 - e. Depict gang affiliation
 - f. Contain language or symbols that demean an identifiable person or group or otherwise infringe on the rights of others
 - g. Cause or are likely to cause a substantial or material disruption to school activities or the orderly operation of the school
 - h. Contain rude, disrespectful, or discourteous expressions inconsistent with civil discourse and behavior
 - i. Constitute bullying, cyber-bullying, harassment, or intimidation in violation of Policy 1040, Safe School Environments.

Reasonable exceptions to this provision may be made for students conducting educational research under the direction of a teacher. Specific permission must be granted regarding the nature of the research to be conducted and the type of files related to that research which might be accessed/created.

5. Students may not access online games without the permission of a faculty member.
6. Students in grades pre-K through 8 may not search the Internet independently. Searches conducted by students in grades pre-K through 8 must be confined to approved online databases.
7. Where independent access to the Internet is assigned (see section II.B.8), parent permission is required, and both the student and the parent or guardian must sign the school system use of Internet permission form. By signing this form, the student agrees to provisions of Policy 8080, these procedures, and current user guidelines. Students who are granted independent access under this provision may use school system computer technology to access individual e-mail accounts for school-related purposes during non-instructional periods of the day provided such use is in compliance with the policy (note Standards D and E).
8. Students may not install software on school system equipment unless directed to do so by an instructor or administrator.

III. Individual Technology Accounts

- A. All employees shall have individual technology accounts. Access privileges for employees to school system computer technology should be granted on an as-needed basis and subject to established guidelines. When employees are transferred and/or professional responsibilities change, appropriate supervisors are responsible for reviewing access privileges and ensuring that access is terminated or modified as appropriate. The Office of Human Resources is responsible for notifying the System Administrator when employment is terminated so that individual accounts and access privileges can be cancelled. An extension of up to 30 days may be granted for transition purposes, except that when the circumstances surrounding termination are such that there may be a threat to school system computer technology, the employee's supervisor is responsible for taking immediate steps to contact the System Administrator and terminating access.
- B. The creation of individual accounts and access privileges for other users shall be strictly limited and subject to guidelines established for that purpose by the System Administrator. When the purpose for creating such accounts has ended,

the authorizer is responsible for notifying the System Administrator that the account should be cancelled and access privileges should be terminated.

IV. Violation of Policy

- A. If a violation of Policy 8080 and these procedures is suspected, the violation should be reported to the appropriate administrator or supervisor for investigation.
- B. In cases that may be criminal in nature (threats, stalking, harassment, etc.), any investigation should be conducted in consultation and cooperation with the Security Coordinator and the System Administrator.

ADOPTED: November 26, 2002

AMENDED: January 21, 2003

May 10, 2007

EFFECTIVE: July 1, 2007