



---

## **I. Policy Statement**

The Board of Education believes that as new technologies change the ways that information may be accessed, communicated, and transferred, those changes provide new opportunities and responsibilities for students and employees. The Board expects that all users will operate Howard County Public School System (HCPSS) technology in a responsible, civil, ethical, and appropriate manner. The Board expects that employees will integrate thoughtful, sustainable use of technology throughout the curriculum and instruction. The Board also expects that employees will apply technology appropriately in the tasks associated with their responsibilities and positions.

The Board is committed to providing appropriate access to technology for employees and students in furtherance of the educational goals and objectives of the school system. The Board recognizes that HCPSS technology must be protected from unauthorized access, modification, destruction, or distribution, whether accidental or intentional.

## **II. Purpose**

The purpose of this policy is to provide guidance related to maintaining the integrity, safety, and proper use of technology provided by the HCPSS.

## **III. Definitions**

Within the context of this policy, the following definitions apply:

- A. Account Credentials – Any data or object used specifically for the purpose of gaining access (authenticating) to an electronic system, usually a username and password combination.
- B. Computer System – Any electronic medium that can execute a set of instructions designed to perform a specified task.
- C. Network – The physical means of transmitting data between computer systems; includes wired and wireless technologies.
- D. Online Resource – Any electronic system which can be accessed remotely for the purpose of viewing or manipulating data which can exist on the Internet, on the wide area network or on the local area network.

- E. Software – Any application that can be executed on a computer system, server, or other electronic device.
- F. Systems Administrator – The person responsible for implementing, managing, and maintaining HCPSS technology.
- G. Technology – Electronic resources including, but not limited to, computer systems, servers, telephones, facsimile equipment, cellular phones, portable electronic devices, network infrastructure, online resources, e-mail, and all data stored or transmitted electronically.
- H. Technology Security Analyst – The person responsible for ensuring that all HCPSS technology is implemented securely in compliance with all legal and regulatory mandates regarding electronic systems.
- I. Users – Any persons using HCPSS technology, including but not limited to, all employees, volunteers, interns, contractors, parents, non-school group members, and students.

#### **IV. Standards**

- A. Access to HCPSS technology will be provided in accordance with the procedures associated with this policy.
- B. All content transmitted using HCPSS technology is subject to Policy 1040 Safe School Environments; Policy 1060 Bullying, Cyberbullying, Harassment, or Intimidation; Policy 3040 Technology Security; Policy 7030 Employee Discipline; Policy 9050 Student Records and Confidentiality; Policy 9200 Discipline; and the Student Code of Conduct.
- C. HCPSS technology is intended for instructional use and school-related business. It is not intended for 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. HCPSS technology is available for personal use so long as the use does not interfere with student or employee work, cause disruptions to the school or work environment, result in additional costs, or violate HCPSS policies or applicable laws.
- D. Access to HCPSS technology granted by virtue of the user's status as an employee, student, volunteer, intern, or contractor will be terminated when the relationship is terminated or the purpose is fulfilled.
- E. All software, including online resources, 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.

- F. Student records which are maintained electronically must be maintained in a confidential and secure manner in accordance with Policy 9050 Student Records and Confidentiality.
- G. HCPSS has the right to monitor, access, archive, audit, purge, or disclose the contents of electronic communications, files, and other material created, stored, or accessed using HCPSS technology. Access must be authorized by the Superintendent/Designee. If a review shows violation of this or other policies, appropriate actions will be taken.
- H. Users assume full responsibility for any and all electronic content they may generate, access, or download, and shall have no privacy expectations in regard to this content or to audit logs while using HCPSS technology.
- I. The Board and HCPSS are committed to the implementation of the Children's Internet Protection Act (CIPA). In order to comply with CIPA, technology which attempts to filter abusive, libelous, obscene, offensive, profane, threatening, sexually explicit, pornographic, illegal, or other inappropriate material will be employed.
- J. Reassignment of technology between schools, offices, or other physical locations must be approved by the Systems Administrator and must be in compliance, when applicable, with Policy 4040 Fixed Assets.
- K. HCPSS regularly re-evaluates specific technology standards for computers. These standards establish the technologies that may be employed within HCPSS.
- L. Costs incurred due to negligence or misuse that result in malicious destruction, or theft of HCPSS technology will be the financial responsibility of the negligent person(s).
- M. Users are expected to use HCPSS technology in a responsible, civil, ethical, and legal manner.
- N. Notice of the provisions of this policy and user responsibilities will be communicated to all students, parents, employees, and users of HCPSS technology.

- O. Failure by any user to comply with this policy will result in the temporary or permanent termination of technology access privileges, in addition to any applicable disciplinary action or financial obligation.
- P. In cases of potential harm to an individual, “duty to inform” obligations will be employed.

**V. Compliance**

- A. The Superintendent/Designee will establish guidelines and appropriate acceptance forms for the acceptable use of technology.
- B. The Superintendent/Designee is responsible for communicating the provisions of this policy annually through customary channels.
- C. The Superintendent/Designee is responsible for reviewing this policy at least every three years and recommending it for revision as necessary.
- D. The Systems Administrator/Designee must approve software before installation on HCPSS technology.
- E. Principals and supervisors are responsible for notifying students, families, and employees in their schools and offices of the provisions of this policy.
- F. Principals and supervisors are responsible for notifying students, families, and employees in their schools and offices of all end-of-year and end-of-employment check-out procedures.
- G. The Office of Human Resources is responsible for notifying the Technology Security Analyst of change of employment status for any employee.
- H. The Technology Security Analyst is responsible for establishing prudent measures to safeguard the security of HCPSS technology in accordance with Policy 3040 Technology Security.
- I. Using established procedures, the Technology Security Analyst/Designee will modify account privileges based on changes to employment status.
- J. The Office of Community Services is responsible for notifying individuals or organizations seeking to use school system computer technology as part of an agreement to use school system facilities (Policy 10020 Use of School Facilities by Non-School Groups) of the provisions of this policy.

**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 1060 Bullying, Cyberbullying, Harassment, or Intimidation  
Policy 3040 Technology Security  
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  
HCPSS Internet Use Permission Form  
Student Code of Conduct

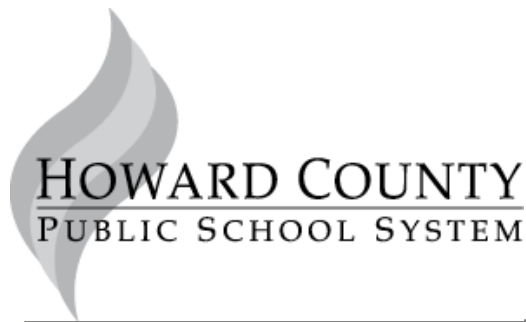
ADOPTED: November 26, 2002

AMENDED: January 21, 2003

May 10, 2007

March 11, 2010

EFFECTIVE: July 1, 2010



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

Effective: July 1, 2010

---

**I. Dissemination of Information**

- A. Notification of the provisions of this policy and these implementation procedures will be given annually to all students, families, employees, and service providers. Methods may include:
1. Announcements in schools over the public address system at the beginning of the school year and at other times as appropriate
  2. Publications in school and system newsletters, handbooks, and other documents
  3. Notification posted in areas that provide access to technology (e.g., media center, computer lab)
  4. Notification posted on school and system websites
  5. Reviews for students by classroom teachers, media specialists, or other appropriate employees
  6. Incorporation, whenever possible and appropriate, into the process of accessing software and/or files.
- B. Principals are responsible for notifying all students, families, employees, volunteers, interns, and contractors in their schools of the responsibilities of users of Howard County Public School System (HCPSS) technology and of guidelines for network activities at the beginning of the school year, with reminders throughout the year.
- C. The Use of School Facilities Office is responsible for notifying individuals or organizations seeking to use HCPSS technology as part of an agreement to use HCPSS facilities under Policy 10020 Use of School Facilities by Non-School Groups of the provisions of this policy and these implementation procedures.
- D. Department supervisors are responsible for notifying those under their supervision of the provisions of this policy and these implementation procedures annually.

## II. Responsibilities of Use

- A. All users of HCPSS technology must comply with the following:
1. Users are responsible for taking reasonable precautions to protect HCPSS-owned technology equipment against damage and/or theft.
  2. Users are responsible for using HCPSS technology, whether onsite or remotely, in an ethical, responsible, and legal manner.
  3. Users will 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 not engage in unauthorized activities. These include, but are not limited to:
    - a. Accessing data for which users do not have privilege
    - b. Accessing information prohibited by the provisions of this policy and these implementation procedures
    - c. Knowingly deploying computer viruses or software with malicious intent
    - d. Violating copyright laws or the privacy rights of others
    - e. Plagiarism
    - f. Accessing technology via another user's account credentials or facilitating unauthorized access
    - g. The destruction of HCPSS technology or the unauthorized manipulation of data, or disrupting network activity
    - h. Circumventing or disabling technology protection measures put in place by the Technology Security Analyst
    - i. Using technology on the HCPSS network which is not in compliance with current HCPSS computer standards unless approved in writing by the Superintendent/Designee.
  5. Users are responsible for securing and safeguarding data stored on HCPSS technology.
- B. All employees, volunteers, interns, and contractors using HCPSS technology must comply with the following:
1. Employees, volunteers, interns, and contractors are to use HCPSS technology in a responsible, ethical manner consistent with their professional responsibilities.

2. Employees, volunteers, interns, and contractors will not create, access, download, store, or print content that is 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 HCPSS e-mail system. Employees are responsible for all e-mail sent from their accounts.
4. Employees, volunteers, interns, and contractors 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. Employees, volunteers, interns, and contractors responsible for central office, departmental, or school electronic publications such as websites and newsletters will ensure that:
  - a. Principals or department supervisors approve the content of all publications
  - b. Only approved users post content to HCPSS online resources
  - c. Written permission is obtained and kept on file for all 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 monitored for appropriateness and, where applicable, comply with Policy 4010 Donations
  - f. Student publications are subject to Policy 9030 Student Publications and Productions.
6. Employees, volunteers, interns, and contractors assigning directed Internet use for students will prescreen online 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.
7. Independent Internet activities are permitted at the high school level only. Employees assigning independent Internet activities will ensure that such activities are applicable to the curricular needs of the assignments and the developmental levels of the students and that signed HCPSS parent permission forms for independent student 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.6).

8. To ensure student safety and acceptable standards of computer use, it is important that all students be given instruction on the acceptable use of technology. Principals are responsible for designating the persons who will instruct the students in the following topics:
  - a. The contents of this policy and these implementation procedures
  - b. Procedures for accessing appropriate online resources
  - c. Provisions contained in the HCPSS Internet Use permission forms (high school students only)
  - d. Copyright issues
  - e. Privacy issues
  - f. Safety and security guidelines, including the use of the Internet
  - g. Making appropriate judgments about locating and using information that matches the learner's instructional level and the learning objectives of the assignment
  - h. Discriminating among types of information sources and assessing the appropriateness of using the Internet as a resource for a specific learning activity
  - i. Rigorous appraisal of the source.
9. When sending confidential material electronically, the sender must alert the recipient that the message contains confidential student information in accordance with FERPA (Family Educational Rights and Privacy Act). The use of student identifiers must be avoided in e-mail.
10. Online resources which support collaborative discussions (i.e., Wikis, blogs, instant messaging, threaded discussions, social networking sites) must be approved through the software approval process (Policy 8040 Selection of Instructional Materials) prior to use.
11. Online resources used for instruction and associated student-generated work must have the ability to monitor 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 online resources.
12. All employees, volunteers, interns, and contractors will be required to authenticate to HCPSS computers using individual account credentials. Access privileges for employees to HCPSS technology will 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 Technology Security Analyst of

change of employment status for any employee so that individual accounts and access privileges can be cancelled.

- C. All students using HCPSS technology must comply with the following:
1. Students are responsible for their behavior while utilizing school system technology.
  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 or legal guardian of the student whose information is being posted or transmitted is required.
  3. Students may not use HCPSS technology unless directed to do so by an instructor or administrator or unless the technology has been previously approved for student use.
  4. Students will not create, access, download, store, or print content that:
    - a. Depicts profanity, obscenity, the use of weapons, or violence
    - b. Promotes use of tobacco, drugs, alcohol, or other illegal or harmful products
    - c. Contains sexually suggestive messages
    - d. Is sexually explicit or obscene
    - e. Depicts gang affiliation
    - f. Contains language or symbols that demean an identifiable person or group or otherwise infringe on the rights of others
    - g. Causes or is likely to cause a disruption to school activities or the orderly operation of the school
    - h. Contains rude, disrespectful, or discourteous expressions inconsistent with civil discourse or behavior
    - i. Constitutes bullying, cyberbullying, harassment, or intimidation in violation of Policy 1040 Safe School Environments, or Policy 1060 Bullying, Cyberbullying, Harassment, or Intimidation.

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 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.
6. Where independent access to the Internet is assigned (see section II.B.7), parent permission is required, and both the student and the parent or legal guardian must sign the HCPSS Internet Use permission form. By signing this form, the student agrees to the provisions of this policy.

### **III. Violation of Policy**

- A. Any employee who suspects a violation of this policy or these implementation procedures must report the alleged violation to the appropriate administrator or supervisor for investigation.
- B. The administrator or supervisor must report the suspected violation to the Security Coordinator, who is the staff member responsible for the security services within HCPSS.
- C. In cases that may be criminal in nature (threats, stalking, harassment, etc.) or that may pose a safety threat, an investigation should be conducted in consultation and cooperation with the Security Coordinator, Technology Security Analyst, and the Systems Administrator.
- D. In cases of potential harm to an individual, there is a “duty to warn” obligation which requires immediate follow-through and communication with the individual in danger and others who are in a position to protect that individual from harm.

ADOPTED: November 26, 2002

AMENDED: January 21, 2003

May 10, 2007

March 11, 2010

EFFECTIVE: July 1, 2010