HOWARD COUNTY
PUBLIC SCHOOL SYSTEM

BOARD OF EDUCATION

POLICY 8080
RESPONSIBLE USE OF
TECHNOLOGY AND SOCIAL MEDIA

Effective: July 1, 2016

I. Policy Statement

The Board of Education of Howard County is committed to providing equitable access to technology and social media to further the strategic goals of the Howard County Public School System (HCPSS). The Board believes that technology should be leveraged to improve instruction, business operations, and communications. The Board encourages the use of social media to enhance student and stakeholder engagement, facilitate collaborative communications, and increase global connections. The Board believes that as technology changes the ways that information is accessed, stored, communicated, and transferred, those changes provide new opportunities and responsibilities. The Board expects that all individuals will act in a responsible, civil, ethical, and appropriate manner when using technology for HCPSS-sanctioned activities.

II. Purpose

The purpose of this policy is to define expectations for:

- The responsible use of technology and social media for HCPSS-sanctioned activities.
- The responsible use of technology and social media to enhance the education process and improve systemwide communications efforts.
- Maintaining the safety and privacy of individuals.

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. Authentication – Verification of an individual's identity through username/password or other mechanism.

C. Digital Tool – Any website, application (app), or software that requires an account.

D. Network – The means of transmitting data between computer systems; includes wired and wireless technologies.

E. Online Resource – Any website, application (app), or software that does not require an account.

F. Personally Identifiable Information (PII) – Any information that, alone or in combination, would make it possible to identify an individual with reasonable certainty.

G. Personal Social Media Account – A social media account created by an employee to conduct non-HCPSS sanctioned activities.

H. Professional Social Media Account – A social media account created by an employee for HCPSS-sanctioned activities.

I. Social Media – Digital tools that enable users to create and share content or to participate in social networking such as, blogs, microblogs, Internet forums, wikis, and social bookmarking. Email is excluded from this definition.

J. Software – Any application or script that can be executed on a computer system, server, or other electronic device.

K. Technology – Electronic devices, network infrastructure, or any applications including but not limited to software, online resources, digital tools, social media, and email.

L. Terms of Service – Rules and notification written by a service provider that individuals must agree to in order to use the service.

M. Third Party Service – Digital tool in which individuals or schools agree to the generic terms of services and privacy policies of a service provider. The individuals or schools create accounts.

IV. Standards

A. General

1. Notice of the provisions of this policy and individual responsibilities will be communicated to all students, parents, employees, and other users of HCPSS technology.

2. Access to technology will be provided in accordance with the procedures associated with this policy and in accordance with Policy 3040 Technology Security.

3. All content transmitted through technology for HCPSS-sanctioned activities is subject to all relevant HCPSS Board policies.

4. The personal use of technology, digital tools, and social media may not interfere with student or employee work, cause disruptions to the school or work

environment, result in additional costs to the HCPSS, or violate HCPSS policies or applicable laws.

B. Compliance

1. Electronic student and personnel records, as well as other student records and personally identifiable information, will be kept confidential and secure in accordance with Policy 9050 Student Records, Policy 7010 Personnel Records, and the federal law, Family Educational Rights and Privacy Act (FERPA).

2. All digital tools and social media used with students for HCPSS-sanctioned activities will be authorized before use in accordance with Policy 8040 Selection of Instructional Materials.

3. HCPSS technology and authorized digital tools and social media are accessible for instructional use and HCPSS-sanctioned activities consistent with current student and employee roles and instructional requirements.

4. All HCPSS technology, digital tools, and social media will comply with licensing and fair use agreements and applicable policies. Individuals will abide by the Terms of Service and privacy policy.

5. Digital tools and social media that do not publish terms of service and privacy policies consistent with federal and state student privacy protections may not be used for HCPSS-sanctioned activities.

6. All authorized digital tools will comply with the federal law, the Children's Online Privacy and Protection Act (COPPA), and the Annotated Code of Maryland, Education Article, §4-131, Student Data Privacy Act of 2015.

7. In order to comply with the federal law, Children's Internet Protection Act (CIPA):

   a. The HCPSS will deploy technology that attempts to filter abusive, libelous, obscene, offensive, profane, threatening, sexually explicit, pornographic, illegal, or other inappropriate material that is harmful to minors.

   b. Employees will monitor online HCPSS-sanctioned student activities including social media and digital tools, to the extent practical.

8. In order to comply with federal and state laws, the Protecting Children in the 21st Century Act, and Grace's Law, Misuse of Interactive Computer Service, staff will provide ongoing instruction to students concerning responsible, appropriate, and civil online behavior, including interacting with other individuals on social networking websites and in chat rooms, and regarding cyberbullying awareness and response.

9. In conformance with the Maryland User Name and Password Privacy Protection and Exclusion Act, Annotated Code of Maryland, Labor and Employment Article, §3-712, staff is prohibited from requesting or requiring an employee or applicant for employment to disclose any account credentials used for accessing a personal social media account or service.

C. Professional Use

1. Professional social media accounts created by employees are the property of the HCPSS.

2. An employee must relinquish information necessary to maintain a professional social media account and may no longer access the account if the employee's job responsibilities change or employment is discontinued through resignation, retirement, termination, or any other cause.

3. Reassignment of technology between schools, offices, or other physical locations will be approved by the Superintendent/Designee and will be in compliance, with Policy 4040 Fixed Assets.

D. Student Use

1. The HCPSS will not mandate that students provide their own technology at school.

2. To ensure accessibility and equal educational opportunities, employees using supplemental digital tools and social media as part of the instructional experience will provide an alternative for students whose parents do not accept the Terms of Service or privacy policy with the exception of HCPSS essential curricular digital tools.

E. Accountability

1. In accordance with Grace's Law and in cases of probable or potential harm to an individual, appropriate follow-through and communication with the individual in danger and others who are in a position to protect that individual from harm including, but not limited to law enforcement, if necessary, must be undertaken by the individual who discovers the probable or potential harm.

2. When student disciplinary investigations lead to searches and seizures on school property that involve technology, these searches and seizures will take place in accordance with the Annotated Code of Maryland, Education Article, Section 7-308 and Policy 9260 Student Search and Seizure.

3. The destruction or theft of HCPSS technology as the result of negligence or misuse will be the financial responsibility of the responsible individual(s).

4. Individuals assume full responsibility for personally-owned technology devices; therefore, the HCPSS is not responsible for any personally-owned technology devices.

5. Digital tools and social media used for HCPSS-sanctioned activities may be monitored for appropriate use. The HCPSS may also access, monitor, archive, audit, purge or disclose the public contents of material created, stored or accessed through personal digital tools and social media accounts when possible and permitted by law.

6. The HCPSS reserves the right to enable or disable interactive features on social media and to remove content inconsistent with the stated purpose, mission, and guidelines posted for the use of the social media.

7. Failure by any individual to comply with this policy may result in the temporary or permanent termination of technology access privileges, in addition to any applicable disciplinary action or financial obligation.

V. Responsibilities

A. The Superintendent/Designee, in coordination with community recommendations from appropriate stakeholders, will establish guidelines for the responsible use of technology and social media.

B. The Superintendent/Designee will communicate the provisions of this policy annually through customary channels.

C. The Superintendent/Designee will review this policy at least every three years and will recommend revision as necessary.

D. The Superintendent/Designee will establish prudent measures to safeguard the security of HCPSS technology in accordance with Policy 3040 Technology Security.

E. The Superintendent/Designee will establish the process for authorizing digital tools for use during HCPSS-sanctioned activities.

F. The Superintendent/Designee will maintain a presence on social media for the HCPSS.

G. The Superintendent/Designee will notify all technology users of all provisions of this policy.

H. The Office of Human Resources will notify the Superintendent/Designee of change of employment status for any employee.

I. Using established procedures, the Superintendent/Designee will modify account privileges based on changes to employment status.

J. Principals and supervisors will notify students, families, and employees in their schools and offices of all end-of-year and end-of-employment checkout procedures.

K. Principals and supervisors will notify all technology users in their schools and offices of all provisions of this policy.

L. Staff will provide information to students regarding digital citizenship, as appropriate.

M. The Office of Use of School Facilities will notify 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) 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

Children's Online Privacy Protection Act of 1998, 15 U.S.C. §6501 (COPPA)
Electronic Communications Privacy Act, 18 U.S.C. §2701-2711
Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232(g)
Protecting Children in the 21st Century Act, 47 C.F.R. §§54.520(c)(1)(i) and 54.520(c)(2)(i)
Section 504 of the Rehabilitation Act of 1973, 20 U.S.C. §794(d)
Title XVII, Children's Internet Protection Act, 47 U.S.C. §254(h) (CIPA)
The Annotated Code of Maryland, Criminal Law Article, §3-805 (Misuse of Interactive Computer Service (Grace's Law))
The Annotated Code of Maryland, Education Article, §4-131, Student Data Privacy Act of 2015
The Annotated Code of Maryland, Education Article, §7-308 (Searches of students and schools)
The Annotated Code of Maryland, Labor and Employment Article, §3-712 (User Name and Password Privacy Protection and Exclusions)

B. Other Board Policies

Policy 1000 Civility
Policy 1040 Safe and Supportive Schools
Policy 1060 Bullying, Cyberbullying, Harassment, or Intimidation
Policy 2070 Ethics
Policy 3040 Technology Security
Policy 4040 Fixed Assets
Policy 4050 Procurement of Goods and/or Services
Policy 4080 Disposition of Property
Policy 7010 Personnel Records
Policy 7030 Employee Conduct and Discipline

Policy 8040 Selection of Instructional Materials
Policy 8060 Resource Speakers
Policy 8120 Testing: State and Local Responsibilities and Protocols
Policy 9020 Students' Rights and Responsibilities
Policy 9030 School-Sponsored Publications and Productions
Policy 9050 Student Records
Policy 9200 Student Discipline
Policy 9260 Student Search and Seizure
Policy 10010 Distribution and Display of Materials and Announcements
Policy 10020 Use of School Facilities

C. Relevant Data Sources
Central Inventory Database

D. Other
HCPSS Device Agreement Form
HCPSS Information Technology Change Management Guideline
HCPSS Student and Parent Handbook
HCPSS Student Code of Conduct

VIII. History

ADOPTED: November 26, 2002
REVIEWED:
MODIFIED:
REVISED: January 21, 2003
May 10, 2007
March 11, 2010
June 27, 2013
June 9, 2016
EFFECTIVE: July 1, 2016

HOWARD COUNTY
PUBLIC SCHOOL SYSTEM

POLICY 8080-IP
IMPLEMENTATION PROCEDURES

RESPONSIBLE USE OF
TECHNOLOGY AND SOCIAL MEDIA

Effective: July 1, 2016

I. Definitions

Within the context of these implementation procedures, the following definitions apply:

A. Forum – A subsection of a social media service facilitating conversations of a group where individuals may have elevated permissions that allow for moderation of posts or comments.

B. Post – Content including but not limited to text, pictures, audio and videos that are added to a social media by an individual.

II. 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. Publications in school and Howard County Public School System (HCPSS) newsletters, handbooks, and other documents.

2. Notification posted on school and HCPSS websites including, but not limited to, the learning management system and the staff communication tool.

3. Periodic announcements in schools over the public address system at the beginning of the school year and at other times as appropriate.

4. Notification posted in areas that provide access to technology (e.g., media center, computer lab, classrooms, and staff workroom).

5. Ongoing notification/reviews for students by classroom teachers, media specialists, and other appropriate employees.

6. Inclusion, whenever possible and appropriate, into the process of accessing digital tools and/or files.

B. Principals will notify all technology users in their schools of the responsibilities of individuals using HCPSS technology and social media and of guidelines for

network activities at the beginning of the school year per Policy 3040 Technology Security, with reminders as necessary.

C. Department supervisors will notify those under their supervision of the provisions of this policy and implementation procedures annually, with reminders as necessary.

D. The Superintendent/Designee will include language in contracts that requires all contractors and vendors to review and comply with this policy and all related policies.

E. The Office of Use of School Facilities will notify individuals or organizations seeking to use HCPSS technology as part of an agreement to use HCPSS facilities under Policy 10020 Use of School Facilities of the provisions of this policy and these implementation procedures.

III. Responsibilities

A. Individual Responsibilities

1. Individuals will adhere to Policy 1000 Civility, Policy 1040 Safe and Supportive Schools, and Policy 1060 Bullying, Cyberbullying, Harassment, or Intimidation when using HCPSS technology or HCPSS digital tools and social media during HCPSS-sanctioned activities.

2. Individuals are required to sign a device agreement form upon assignment of HCPSS-owned technology equipment.

3. Individuals will take reasonable precautions to protect HCPSS-owned technology equipment against damage, theft, and/or loss. If necessary, individuals will follow the appropriate process and/or procedure for reporting damage, theft, and/or loss.

4. Individuals will not engage in unauthorized activities. These include, but are not limited to:

    a. Accessing information for which the individuals do not have privilege.

    b. Knowingly deploying computer viruses or software with malicious intent.

    c. Violating copyright laws or privacy rights of others.

    d. Plagiarizing.

    e. Accessing HCPSS-owned technology via another individual’s account credentials.

f. Damaging HCPSS technology.

g. Circumventing or disabling technology protection measures put in place by the Superintendent/Designee.

5. Individuals will secure and safeguard data stored on HCPSS technology.

6. Individuals using digital tools and social media for HCPSS-sanctioned activities will use the most restrictive privacy settings when appropriate and available.

7. Individuals responsible for electronic content creation and delivery of public communication will adhere to the guidelines set forth by the HCPSS for the generation and access of such public communication.

8. Individuals using HCPSS technology will not intentionally create, access, share, download or print content that:

   a. Depicts profanity, obscenity, the use of weapons, terrorism, 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 HCPSS activities or the orderly operation of the HCPSS.

   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 and Supportive Schools or Policy 1060 Bullying, Cyberbullying, Harassment, or Intimidation.

   j. Reasonable exceptions to this provision may be made for students conducting research under the direction of an instructor and employees completing HCPSS related responsibilities. Specific permission will be granted regarding the nature of the research to be conducted and the type of files related to that research which might be accessed or created.

9. Individuals will authenticate using HCPSS active directory credential assigned to each individual, to HCPSS technology consistent with Policy 3040 Technology Security when using HCPSS-owned or personally-owned devices.

10. The HCPSS has the following expectations for individuals using personally-owned technology during HCPSS-sanctioned activities:

    a. Individuals will use personally-owned devices in accordance with all HCPSS policies. Failure to comply with these polices may result in the removal of temporary or permanent use privileges in addition to any disciplinary action.

    b. Individuals will use devices in a responsible, civil, ethical, and legal manner.

    c. Individuals will assume full responsibility for their personal technology devices and the content stored on these devices.

    d. The HCPSS may, without cause, revoke the privilege of using personal technology devices at any time.

    e. Individuals will ensure that their personal technology devices contain up to date operating system and relevant software patches and anti-malware software.

    f. The HCPSS will not be liable for any costs incurred related to the use of personal technology devices, including but not limited to, usage fees, upgrades, damages, and replacements.

    g. Individuals will have no expectation of personal privacy or confidentiality of any electronic communication when using HCPSS networks.

    h. Personal technology devices will not contain HCPSS licensed applications or software unless approved by the Superintendent/Designee.

    i. Individuals will not store confidential HCPSS information, excluding the device owner's personal information, on personal technology devices.

    j. Individuals will not use personal technology devices to create or access abusive, libelous, obscene, offensive, profane, threatening, sexually explicit, pornographic, illegal, or other inappropriate material during HCPSS-sanctioned activities.

k. Individuals will not use personal technology devices to gain or attempt to gain unauthorized access to any system or information.

l. Individuals will not use personal technology devices to circumvent, modify, or disable technology security measures implemented by the HCPSS. These measures include but are not limited to:

i. Anti-malware software.
ii. Internet content filter.
iii. Privacy settings and/or parental controls.
iv. Network firewalls.
v. Computer and server administrative management software.

m. Personal technology devices placed on the HCPSS network may not disrupt normal network activities.

n. Individuals are responsible for reporting any inappropriate material they receive on personal technology devices.

B. Professional Responsibilities

1. Employees will obtain approval from their administrator/supervisor using the appropriate procedures prior to creating a social media account for HCPSS-sanctioned activities.

2. Employees who change schools or roles in the HCPSS, will inform their administrator/supervisor of their professional social media account.

3. The Superintendent/Designee will review and update guidelines for network activities in all schools.

4. School principals/designees will determine how the guidelines are implemented in their schools with stakeholder feedback from students, staff, and parents.

5. To ensure student safety and acceptable standards of technology use, all students will be given instruction on the responsible use of technology and social media. Principals will designate 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. Copyright issues.

d. Privacy issues, including not sharing personally identifiable information.

e. Safety and security guidelines, including the use of the Internet.

f. Making appropriate judgments about locating and using information that matches the learner's instructional level and the learning objectives of an assignment.

g. Discriminating among types of information sources and assessing the appropriateness of using the Internet as a resource for a specific learning activity.

h. Rigorous appraisal of the source.

i. Digital citizenship.

6. Employees using social media and digital tools with students will ensure that the digital tool appears on an authorized list.

7. Employees selecting online resources will evaluate the resources to ensure that they meet the curricular needs of students and are appropriate for the developmental level of the students.

8. When using social media in the teaching and learning process, employees will:

   a. Configure privacy settings of the social media to limit the visibility of the content to the intended audience.

   b. Inform parents of the social media being used, how their children are being contacted online, and the expectations for appropriate behavior.

   c. Distribute and discuss communication and collaboration guidelines with students prior to using social media.

   d. Adhere to Policy 8060 Resource Speakers when inviting non-HCPSS individuals to collaborate using social media. Access by the non-HCPSS individual will be terminated after the educational purpose has been fulfilled.

9. HCPSS employees will ensure students are authenticating to the network when using HCPSS-owned or personally-owned devices.

10. Employees using digital tools and social media professionally will create an account linked to their HCPSS email address separate from any personal accounts.

11. When using digital tools and social media for professional purposes, employees will identify themselves as an HCPSS employee.

12. Employees will delete or inactivate HCPSS digital tools and social media accounts that are no longer required.

13. Upon request, employees will provide the administrator/supervisor administrative access to any professional social media accounts or forums they have created.

14. Any postings by employees will not reference, link or contain:

    a. Statements that could be viewed as malicious, obscene, threatening or intimidating; that disparage students, employees, parents or community members; or that could be viewed as harassment or bullying.

    b. HCPSS password-protected proprietary items, private, confidential or attorney-client privileged information such as assessments, curriculum, lessons, and personnel issues.

15. Employees are responsible for all communication sent from their accounts. When using electronic accounts to correspond with parents and students, employees will use an approved HCPSS communication system.

16. Employees will ensure the confidentiality and privacy of student, staff and district data. Employees will only share confidential data when directed to do so by their immediate supervisor or administrator and will comply with Policy 9050 Student Records and Policy 7010 Personnel Records.

    a. When sending confidential records electronically, the sender will alert the recipient that the message contains confidential data.

    b. When sending confidential student records electronically, the sender will alert the recipient that the message contains confidential student data in accordance with FERPA (Family Educational Rights and Privacy Act).

17. Principals or supervisors are responsible for the content of all publications created for their schools/departments.

18. HCPSS employees responsible for central office, departmental, or school electronic communications and media will ensure that:

    a. Written permission is obtained and kept on file for all copyrighted material or student work used in publications.

    b. When parents have requested that their students are not photographed, those students do not appear in HCPSS publications, including social media. This restriction does not apply to extracurricular events that are open to the public.

c. Commercial links and/or advertising are monitored for appropriateness and, where applicable, comply with Policy 4010 Donations and Policy 4020 Fund Raising.

d. Student publications comply with Policy 9030 School-Sponsored Publications and Productions.

19. Employees who moderate HCPSS-sanctioned forums may edit or delete posts and will document the posts that are edited or deleted for future reference.

20. Employees will not use HCPSS logos or trademarks for personal use.

21. Periodically, HCPSS may approve pilot studies to explore new learning materials, approaches or innovations. When new ideas, devices or methods are being piloted, exceptions to this policy may be made by Superintendent/Designee.

C. Student Responsibilities

Students may only use technology during HCPSS-sanctioned activities when authorized to do so by an instructor or administrator.

IV. Violation of Policy

A. Any individual who suspects a violation of this policy or these implementation procedures will report the alleged violation to the appropriate administrator or supervisor for investigation.

B. The administrator or supervisor will report the suspected violation to the Superintendent/Designee for further investigation and potential disciplinary action.

C. In cases that may be criminal in nature (threats, stalking, harassment, etc.) or that may pose a safety threat, an investigation will be conducted in consultation and cooperation with the Superintendent/Designee.

D. In cases of probable or potential harm to an individual, appropriate follow-through and communication with the individual in danger and others who are in a position to protect that individual from harm including, but not limited to law enforcement, if necessary, must be undertaken by the individual who discovers the probable or potential harm.

E. Suspicious activity can be reported anonymously through the HCPSS main website - Reporting Fraud and Abuse. Reports can also be emailed directly to abuse@hcpss.org.

V. History

ADOPTED: November 26, 2002
REVIEWED:
MODIFIED:
REVISED: January 21, 2003
May 10, 2007
March 11, 2010
June 27, 2013
June 9, 2016
EFFECTIVE: July 1, 2016