HOWARD COUNTY
PUBLIC SCHOOL SYSTEM

BOARD OF EDUCATION

POLICY 8080
RESPONSIBLE USE OF TECHNOLOGY, DIGITAL TOOLS, AND SOCIAL MEDIA

Effective: July 1, 2020

I. Policy Statement

The Board of Education of Howard County is committed to providing equitable access to technology and digital tools 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 acknowledges that social media can be used to enhance student and stakeholder engagement, facilitate collaborative communications, and increase global connections. The Board expects that all individuals will act in a responsible, civil, ethical, and appropriate manner when using technology, digital tools, and social media.

II. Purpose

The purpose of this policy is to define expectations for individuals regarding the responsible use of technology, digital tools, and social media for HCPSS-sponsored programs.

III. Definitions

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

A. Account Credentials – Any data or object used for the purpose of gaining access (authenticating) to an electronic system, usually a username and password combination.

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

C. Confidential Data – Individual, fact, statistic or item of information whereby access is restricted based on least privilege.

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

1. Essential Digital Tool – A Superintendent/designee-approved digital tool necessary to deliver educational programs and operational services.

2. Supplemental Digital Tool – A Superintendent/designee-approved digital tool used as non-essential enrichment to students' educational experience.

E. Digital Resource – Teacher-selected digital content that does not require a student and/or teacher account to access.

F. HCPSS-Sponsored Program – An activity, event or meeting developed or organized by HCPSS with the knowledge and approval of the associated school principal and/or Superintendent/designee that is under the direction and control of an authorized HCPSS employee, where HCPSS assumes full responsibility and liability for the program, event or action. This includes the instructional day.

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

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

I. Parent – Any one of the following, recognized as the adult(s) legally responsible for the student:

1. Biological Parent – A natural parent whose parental rights have not been terminated.

2. Adoptive Parent – A person who has legally adopted the student and whose parental rights have not been terminated.

3. Custodian – A person or agency appointed by the court as the legal custodian of the student and granted parental rights and responsibilities.

4. Guardian – A person who has been placed by the court in charge of the affairs of the student and granted parental rights and responsibilities.

5. Caregiver – An adult resident of Howard County who exercises care, custody or control over the student but who is neither the biological parent nor legal guardian, as long as the person satisfies the requirements of the Education Article, §7-101 (c) (Informal Kinship Care) or has been issued a U.S. Department of Health and Human Service's Office of Refugee Resettlement (ORR) Verification of Release form entering into a custodial arrangement with the federal government.

6. Foster Parent – An adult approved to care for a child who has been placed in their home by a state agency or a licensed child placement agency as provided by the Family Law Article, §5-507.

J. Personal Technology Device – Any non-HCPSS device that may be used to send or receive data via voice, video or text. This includes, but is not limited to, mobile phones, e-readers, tablets, personal computers, wearable technology, video recorders or other devices equipped with microphones, speakers and/or cameras.

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

L. Social Media – Applications or platforms that enable users to create and share content, or to participate in social networking. Email and essential digital tools are excluded from this definition.

1. HCPSS Social Media Account – Created and/or used by an employee or office for HCPSS business or HCPSS-sponsored programs.

2. Personal Social Media Account – Used by an employee for non-HCPSS business.

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

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

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

IV. Standards

A. General

1. The 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 HCPSS, or violate applicable laws or Board of Education policies, including but not limited to Policy 1000 Civility; Policy 1040 Safe and Supportive Schools; Policy 1060 Bullying, Cyberbullying, Harassment, or Intimidation; Policy 2070 Ethics; Policy 3040 Technology Security; Policy 3060 Student Data Governance and Privacy; and Policy 7030 Employee Conduct and Discipline.

2. An employee's use of personal social media may not disrupt the work/school environment, impair their ability to perform their HCPSS duties effectively, undermine supervisory authority, and/or compromise working relationships within HCPSS schools and offices. Any postings by employees will not reference, link or contain 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.

3. Access to technology and digital tools will be provided in accordance with this policy and with Policy 3040 Technology Security and Policy 3060 Student Data Governance and Privacy.

4. All content transmitted through technology for HCPSS business, HCPSS-sponsored programs, and/or school-sponsored programs is subject to all relevant Board policies.

5. All digital tools used with students for HCPSS-sponsored programs will be authorized before use in accordance with Policy 3060 Student Data Governance and Privacy and Policy 8040 Selection of Instructional Materials.

6. HCPSS technology provided for instruction will be accessible to all students,

7. HCPSS technology provided will be consistent with current student and employee roles and instructional requirements.

8. Individuals will access HCPSS technology and digital tools using their own assigned account credentials, in accordance with Policy 3040 Technology Security.

9. Individuals who use HCPSS-owned technology will take reasonable precautions to protect 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.

10. Individuals who use HCPSS technology will secure and safeguard data stored, in accordance with Policy 3040 Technology Security.

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

12. Individuals assume full responsibility for their personal technology devices, including but not limited to, usage fees, upgrades, damages, and replacements.

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 3060 Student Data Governance and Privacy, Policy 7010 Personnel Records, Policy 9050 Student Records, and the Family Educational Rights and Privacy Act (FERPA).

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

3. Digital tools approved for use with HCPSS-sponsored programs will comply with Policy 3060 Student Data Governance and Privacy as well as federal, state, and local student data privacy protections, including 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.

4. In order to comply with the Children's Internet Protection Act (CIPA):

a. 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. To the extent practical, employees will monitor students' use of essential digital tools.

5. In order to comply with the Protecting Children in the 21st Century Act, and Grace's Law 2.0, Misuse of Electronic Communication, employees will provide instruction to students concerning responsible, appropriate, and civil online behavior, including interacting with other individuals on social media, and cyberbullying awareness and response. (Policy 1060 Bullying, Cyberbullying, Harassment, or Intimidation.)

6. In conformance with the Maryland Username and Password Privacy Protection and Exclusion Act and the Annotated Code of Maryland, Labor and Employment Article, §3-712, employees are 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. Employee Use – Technology

1. When using digital tools for instructional purposes or for HCPSS-sponsored programs, employees will only use HCPSS essential digital tools and supplemental digital tools.

2. When using supplemental digital tools for instructional purposes or for HCPSS-sponsored programs, employees will notify parents of the tools they have chosen and parents will have the opportunity to opt-out of their student's use of these tools.

3. When using digital resources, employees will adhere to Policy 8040 Selection of Instructional Materials.

4. When using any digital tools and/or resources, employees will provide alternative supports and materials when needed.

D. Employee Use – Social Media

1. HCPSS social media accounts are the property of HCPSS.

2. Prior to creating an HCPSS social media account, employees must obtain their principal or supervisor's written approval and provide administrative access to the account.

3. If an employee's job responsibilities change or employment is discontinued, the employee's supervisor will reset administrative access to any social media accounts to which the employee had access.

4. When using personal social media accounts, employees will adhere to Standard A.2. and will not share information to which they have access only as part of their official responsibilities as an HCPSS employee.

    a. This includes, but is not limited to, personally identifiable student or employee information and photographs.
    b. This does not include sharing publicly available information.

E. Student Use – Technology

1. When using online technology at any HCPSS location, students must authenticate to the HCPSS network, consistent with Policy 3040 Technology Security.

2. When technology is necessary for instruction, HCPSS will provide devices for student use.

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

4. HCPSS permits students to bring personal technology devices to school, according to the following rules:

    a. Elementary Schools – Students will keep personal technology devices in backpacks during the school day, unless otherwise authorized by school administrators or instructional staff.

    b. Middle Schools – Students:

        i. Students will not use personal technology devices during non-instructional time, to include but not limited to transition between classes, lunch, recess, or in bathrooms.

        ii. A school administrator may, on occasion, authorize the use of personal technology devices for special events and/or for positive behavioral supports and interventions.

    c. High Schools – Students:

        i. May only use personal technology devices during classroom instruction when allowed by instructional staff; and

ii. May use personal technology devices during non-instructional time (transitions between classes, lunch or special events), unless prohibited by school administrators or instructional staff.

F. Student Use – Social Media

1. HCPSS will not mandate that students create or use social media for instruction or for HCPSS-sponsored programs.

2. Students will not create HCPSS social media accounts.

G. Accountability

1. In accordance with Grace's Law 2.0 and Policy 1040 Safe and Supportive Schools, a person who discovers probable or potential harm to an individual must take appropriate measures to communicate with that individual and others who are in a position to protect them from harm, including but not limited to law enforcement.

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 personal technology devices; therefore, HCPSS is not responsible for any personal technology devices.

5. Essential digital tools and HCPSS social media accounts will be monitored for appropriate use. HCPSS may also monitor personal social media accounts and supplemental digital tools to the extent practical.

6. HCPSS reserves the right to enable or disable interactive features on HCPSS social media accounts, and to remove content inconsistent with the stated purpose, mission, and guidelines posted for the use of 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 review and update, as necessary, guidelines for the responsible use of technology, digital tools, and social media.

B. The Superintendent/designee and principals/designees 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-sponsored programs in accordance with Policy 3060 Student Data Governance and Privacy and Policy 8040 Selection of Instructional Materials.

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

G. Employees will provide information to students regarding digital citizenship as part of HCPSS curriculum.

H. The Superintendent/designee 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 Electronic Communication (Grace's Law 2.0))
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 1020 Sexual Discrimination, Sexual Harassment, and Sexual Misconduct
Policy 1040 Safe and Supportive Schools
Policy 1060 Bullying, Cyberbullying, Harassment, or Intimidation
Policy 2070 Ethics
Policy 3040 Technology Security
Policy 3060 Student Data Governance and Privacy
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
June 25, 2020
EFFECTIVE: July 1, 2020

HOWARD COUNTY
PUBLIC SCHOOL SYSTEM

POLICY 8080-IP
IMPLEMENTATION PROCEDURES

RESPONSIBLE USE OF TECHNOLOGY, DIGITAL TOOLS, AND SOCIAL MEDIA

Effective: July 1, 2020

I. Dissemination of Information

A. Notification of the provisions of this policy and these implementation procedures will be provided annually to all students, families, employees, and service providers through customary channels of communication.

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.

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, when applicable, 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 of the provisions of this policy and these implementation procedures as part of agreements to use HCPSS facilities in accordance with Policy 10020 Use of School Facilities.

II. Responsibilities

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

1. Depicts profanity, obscenity, the use of weapons, terrorism, gang affiliation, and/or violence.

2. Promotes use of tobacco, drugs, alcohol, and/or other illegal or harmful products.

3. Contains sexually suggestive messages, or is sexually explicit or obscene.

4. Contains language or symbols that demean an identifiable person or group or otherwise infringe on the rights of others.

5. Causes or is likely to cause a disruption to HCPSS activities or the orderly operation of HCPSS.

6. Contains rude, disrespectful, or discourteous expressions inconsistent with civil discourse or behavior.

7. Constitutes bullying, cyberbullying, harassment, or intimidation in violation of Policy 1020 Sexual Discrimination, Sexual Harassment, and Sexual Misconduct, Policy 1040 Safe and Supportive Schools, and Policy1060 Bullying, Cyberbullying, Harassment, or Intimidation.

8. 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.

B. Employee Responsibilities

1. Employees assigned an HCPSS mobile technology device for use will adhere to the provisions outlined in the HCPSS Mobile Technology Duties and Obligations Notice. An HCPSS Mobile Technology Device includes laptops, iPads, and cell phones. This does not include desktop computers.

2. Prior to using supplemental digital tools with students, employees will:

   a. Check to ensure the supplemental digital tool is on the HCPSS approved list of digital tools.

   b. Notify parents of the supplemental digital tool and provide parents the opportunity to opt their student out of using the digital tool.

   c. Provide alternative materials for those students whose parents have opted them out of using the digital tool.

3. When using digital resources, employees will:

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

   b. Differentiate among types of information sources and assess the appropriateness of using the internet as a resource for a specific learning activity.

   c. Evaluate resources to ensure that they meet the curricular needs of students and are appropriate for the developmental level of the students.

4. When using social media to incorporate external resource speakers, employees will:

    a. Configure privacy settings of the social media to limit the visibility of the content to the intended audience. Access by the non-HCPSS individual will be terminated after the educational purpose has been fulfilled.

    b. Provide the name and organization affiliation of the speaker(s) and notify students and parents of the social media being used, how students will participate, expectations for appropriate behavior, and collaboration guidelines.

    c. Adhere to Policy 8060 Resource Speakers.

5. When creating and/or using an HCPSS social media account, employees will:

    a. Use an HCPSS email address to create the HCPSS social media accounts.

    b. Delete inactive HCPSS social media accounts.

    c. Adhere to Policy 3060 Student Data Governance and Privacy, Policy 7010 Personnel Records, and Policy 9050 Student Records.

    d. Verify parents have provided permissions for media release (photo approval) and/or student creative work release prior to posting photographs or creative work.

    e. Moderate the account for compliance with this policy, and document and delete comments that are not compliant.

C. Student Responsibilities

1. When using technology, students will adhere to all school rules, regulations, and directives of school employees.

2. During the school day, personal technology devices should be set to silent with notifications turned off.

D. Use of Recording Devices

1. Employees will adhere to parent media release consent regarding photographs, videos, or audio recordings intended for a public audience.

2. Instructional staff will notify parents at the start of each school year if photographs, videos, or audio recordings will be taken as part of HCPSS

curriculum and how they will be used. Staff also will provide a process for parents and/or students to opt-out of these recordings.

3. Volunteers and visitors must have the permission of the school administration prior to photographing and/or video or audio recording during the school day, HCPSS-sponsored programs, and field trips. This does not include extracurricular activities or events open to the public.

III. 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.

IV. References

HCPSS Mobile Technology Duties and Obligations Notice

V. History

ADOPTED: November 26, 2002
REVIEWED:
MODIFIED: July 11, 2019
REVISED: January 21, 2003
May 10, 2007
March 11, 2010
June 27, 2013
June 9, 2016
June 25, 2020
EFFECTIVE: July 1, 2020