

I. Dissemination of Information

- A. Notification of the provisions of this policy and these implementation procedures will be given annually, and as otherwise required, 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. Notifications posted in areas that provide access to technology (e.g., media center, computer lab, classrooms, and staff workroom).
 3. Notifications posted on school and HCPSS websites, including but not limited to, the learning management system and the staff communication tool.
 4. Ongoing notification/reviews for students by classroom teachers, media specialists, or other appropriate employees.
 5. Inclusion, whenever possible and appropriate, into the process of accessing digital tools and/or files.
 6. Periodic announcements in schools over the public address system at the beginning of the school year and at other times as appropriate.
- B. Principals are responsible for notifying all students, families, employees, volunteers, contractors, and interns in their schools of the responsibilities of use of HCPSS technology at the beginning of the school year, with reminders as necessary.
- C. Department supervisors are responsible for notifying those under their supervision of the provisions of this policy and these implementation procedures.
- D. 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 school system facilities (Policy 10020 Use of School Facilities) of the provisions of this policy and these implementation procedures.
- E. The Office of Safety, Environment, and Risk Management in collaboration with the Technology Department and the Division of Accountability is responsible for

providing annual Data Privacy and Security Awareness Training for all staff members.

- F. Security notifications and advisory information will be published for relevant audiences through various media including but not limited the learning management system, the staff communication tool, and HCPSS websites.

II. General Procedures

A. Electronic Communications

1. Individuals will have no expectation of personal privacy or confidentiality of any electronic communication when using HCPSS technology.
2. HCPSS technologies that store or transmit employee data, student record data, financial data, or other legally confidential data will implement appropriate authentication and encryption technologies to prevent unauthorized access or modification.
3. Individuals using HCPSS technology will ensure that both their usage and electronic communications content are in compliance with all other HCPSS policies.

B. Online Testing

1. For security purposes, all online testing will be conducted in accordance with the state, local, and vendor-specific guidelines, policies, and procedures.
2. All data saved to computers and servers for online testing administration and execution will be deleted in accordance with the state, local, and vendor-specific guidelines, policies, and procedures.

C. Security Vulnerability Assessments

1. The Superintendent/Designee will coordinate annual technology security vulnerability assessments consistent with industry best practices and in compliance with regulatory mandates.
2. The HCPSS may contract with third party companies or individuals to perform external security vulnerability assessments and penetration tests.

D. Technology Security Incident Response

1. All HCPSS technology security investigations will be authorized by the Superintendent/Designee.
2. The HCPSS will monitor HCPSS technology for potential security incidents.

3. The HCPSS reserves the right to access, record or, if necessary, remove content stored in an individual's assigned account on HCPSS technology with prior written approval from the Superintendent.
4. The HCPSS reserves the right to restrict or remove any device suspected of contributing to a security incident.
5. The Superintendent/Designee will document all HCPSS technology security investigations using the HCPSS Technology Security Incident Handling Form.
6. The Superintendent/Designee will conduct all HCPSS technology security incident investigations in strict confidence.
7. Investigations into incidents involving a potential breach of an individual's private data will include the following:
 - a. Notifications to individuals will be required if it is determined that an individual's personal information has been breached and misuse has occurred or is likely to occur.
 - b. If 1,000 or more individuals are involved in a breach notification, the HCPSS will also notify each consumer reporting agency as defined by 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notices.
 - c. If misuse is not likely to occur, as in cases where the information breached was protected by encryption and there is no evidence the encryption key had been compromised or disclosed, notifications to individuals will not be required.
 - d. The HCPSS will maintain records on determinations for data breach notifications for three years after the determination has been made.

E. Storage Media Handling and Disposal

1. Access to HCPSS storage media including, but not limited to, floppy disks, magnetic tapes, hard disks, CDs, DVDs, USB memory sticks, etc., will be secured utilizing the least privileges methodology.
2. All service to HCPSS computers and servers will be performed onsite by authorized HCPSS personnel or authorized contractors. If a computer or server must be taken offsite for service, all hard drives, CDs, and DVDs will be removed prior to the equipment leaving the premises. If removal of any/all hard disks, CDs, or DVDs is not feasible, prior approval will be obtained in writing by the Superintendent/Designee to remove the equipment.

3. All HCPSS storage media including, but not limited to, floppy disks, hard disks, CDs, DVDs, USB memory sticks, etc., will be disposed of in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-88.

F. Systems Development Life Cycle

1. All HCPSS applications and systems will be developed or procured in compliance with all legal regulatory mandates.
2. When feasible, all HCPSS systems and applications will employ the latest software versions and patch levels to ensure maximum functionality and security.
3. All HCPSS application training data will not include confidential information.
4. All HCPSS application and system source code will be managed in a controlled, auditable environment.
5. Changes to HCPSS technology will be evaluated, approved, and documented in accordance with the Information Technology Change Management Guideline.
6. Systems will be designated as either critical or non-critical.
7. Disaster Recovery procedures will be maintained and tested for all critical systems.

G. System Security

1. The HCPSS will employ technology security measures, including monitoring, to ensure the confidentiality, integrity, availability, and accountability of its technology and data.
2. Open wireless networks will be configured to notify users of network monitoring capabilities and the provisions of HCPSS Policy 8080 Responsible Use of Technology and Social Media.
3. All publicly accessible systems will be located in a separate dedicated network segment configured to restrict access to internal trusted networks.
4. Publicly accessible critical systems will be monitored by an automated vulnerability assessment system at least weekly to confirm configuration and determine the effectiveness of implemented security controls.

5. Critical systems will maintain audit logs to track user activity and actions that are administratively prohibited. Audit logs will be reviewed at least daily.
6. Individuals will not attempt to circumvent, modify, or disable technology security measures implemented by the HCPSS. These measures include but are not limited to:
 - a. Anti-malware software.
 - b. Internet content filter.
 - c. Microsoft Group Policy and Apple Parental Controls.
 - d. Network firewalls.
 - e. Computer and server administrative management software.
7. Wireless access points will be configured utilizing at least Wi-Fi Protected Access (WPA) encryption. Exceptions will be approved by the Superintendent/Designee.

H. Account Credential Assignment and Use

1. Account Credential Assignment
 - a. HCPSS employees will be assigned individual account credentials once employment with the HCPSS has been verified.
 - b. Students will be assigned individual account credentials once enrollment in the HCPSS has been verified.
 - c. Contractors, volunteers, interns, and others will be assigned individual account credentials upon approval of the Request for Computer User Account Form.
 - d. Password length and complexity requirements will be established for each system in order to prevent unauthorized access to or modification of confidential data.
 - e. Temporary account passwords will be unique to the individual recipient and will be changed by the individual upon next login.
 - f. Account credentials are granted in accordance with an individual's role and will be revoked when the individual's role is fulfilled or terminated.
2. Employee's Individual Account Credential Assignment
 - a. Passwords will not be the same as the account username.
 - b. Passwords will not be shared with others.

- c. Passwords will be a minimum of eight characters consisting of mixed alphabetic and numeric characters.
 - d. Password changes will be required at various intervals, depending on the system.
 - e. Password reuse will be prohibited by not allowing the last 10 passwords to be reused with a minimum of at least two days each.
 - f. Individual application, system, and directory service passwords will expire at least once annually.
 - g. Employee accounts associated with a password will be restricted after six unsuccessful logon attempts.
 - h. All employee accounts will be disabled after 120 days of inactivity unless prior approval is obtained from the Superintendent/Designee.
 - i. The HCPSS reserves the right to modify employee account credentials upon change in employment status, as directed by the Superintendent/Designee.
3. Student Account Credentials
- a. Passwords will not be the same as the account username.
 - b. Passwords will not be shared with others.
 - c. Passwords will be a minimum of six characters consisting of mixed alphabetic and numeric characters. Exceptions may be allowed based on demonstrated need.
 - d. Password changes will be required at various intervals, depending on the system.
 - e. Password reuse will be prohibited by not allowing the last 10 passwords to be reused with a minimum of at least two days each.
 - f. The HCPSS reserves the right to disable student accounts.
4. Shared Account Credentials (credentials used by more than a single individual)
- a. The HCPSS may create shared account credentials in support of specific tasks with the approval of the Superintendent/Designee.

- b. Shared accounts will only be used for the specific tasks for which they were intended.

III. Information Technology Equipment Accountability

- A. Physical inventory of Information Technology Equipment will be performed.
- B. Principals/supervisors will ensure that Information Technology Equipment inventory will be completed on an annual basis.

IV. Violation of Policy

- A. Any individual who suspects a violation of this policy or these implementation procedures will report the alleged violation to an 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: March 11, 2010
REVIEWED:
MODIFIED: August 17, 2017
REVISED: May 9, 2013
 June 9, 2016
EFFECTIVE: August 17, 2017