Calvert County Public Schools
1305 Dares Beach Road
Prince Frederick, MD 20678

Administrative Procedures for Policy #2718 (Instruction) Regarding Responsible and Appropriate Use of Computer Systems and Other Electronic Communications

I. Definitions

A. Computer Systems – All hardware, software, and related technology including wired and wireless networks, and communications equipment such as mobile devices and laptops.

B. Content Filtering – The process of limiting access to portions of the Internet that are inappropriate or may be harmful to users.

C. Educational or Employment-Related Purposes – Those actions directly promoting the educational, instructional, administrative, business, and support services mission of CCPS and related to any instruction, project, job, work assignment, task, or function for which the user is responsible.

D. Electronic Communications – Any media used to communicate electronically, including computers, mobile devices, the Internet, and software, whether the media is owned/leased, or not owned/leased by CCPS.

E. Electronic Data – Facts and information contained in any electronic form including but not limited to files, records, and email.

F. Email – A means or system for transmitting messages electronically; messages sent and received electronically through such means or system.

G. Generative AI: A category of artificial intelligence designed to generate various types of content such as text, images, music, video, computer code, etc. Generative AI models are trained on large datasets and learning patterns, which enable the model to create novel content in response to a prompt that mimics the style or substance of the training data.

H. Hate Speech – Speech or expression, including bullying and cyberbullying, that attacks a person or group on the basis of race, color, national origin, religious beliefs, disability, age, gender, appearance, marital status, sexual orientation, gender identity and expression, family status, or any other association or personal characteristics.

I. Inappropriate Content – Content that violates law or CCPS policies and/or procedures; poses a potential threat to the health and/or safety of students; might reasonably be perceived to advocate student drug, alcohol and/or tobacco use, violence, sex, illegal discrimination, or other illegal activities; contains language or images that are obscene, libelous, slanderous, profane, or derogatory to individuals; or causes, or might reasonably be predicted to cause, substantial disruption of or interference with school activities and/or the school's learning environment.

J. Legitimate Educational Interest – Requiring information to perform one's official duties to serve the needs of Calvert County Public Schools' students and/or staff.

K. Plagiarism – Copying of another's ideas, text, or other creative work, and presenting it as one's own, especially without permission including the use of Generative AI.

L. Social Media – Websites and applications used for social networking.

M. Social Networking – Platforms to build social relations among people who share interests, activities, backgrounds, or real-life connections.

N. Staff – All regular, contracted, and temporary employees of Calvert County Public Schools.

O. System Administrator – The Superintendent's designee responsible for implementing and maintaining the school system's hardware and software infrastructure and related policies, including internal and external access and security.

P. User – Any CCPS staff member, student, or other individual that interacts with CCPS computer systems and/or the CCPS network. Other individuals may include parents, volunteers, and contracted or temporary staff.

Q. Virtual Private Network – Technology that encrypts internet data by creating a secure tunnel between your device and the internet. This secure tunnel disguises your IP address, masks your online activity, and hides your physical location.

II. User Responsibilities

A. Users of the CCPS network and computer systems:

1. Are responsible for taking reasonable precautions to protect school system owned computer systems against damage and/or theft.

2. Are responsible for using computer systems in a responsible, appropriate, ethical, legal, and safe manner.

3. Will access only those network resources for which they have obtained permission, using only the account assigned to them.

4. May only access information and/or computer systems to which they are authorized and that they need for their job responsibilities and/or classroom assignments.

5. Except for directory information as defined by the Family Educational Rights and Privacy Act (FERPA), shall not reveal personally identifiable information about students or employees to any individual or agency unless they have a legitimate educational interest. Disclosure of student and employee information is addressed in Policy 1740: Regarding Ethics, Procedure 1740.6: Regarding Confidentiality, Policy and Procedures 1920: Regarding Records Retention and Disposal, Policy and Procedure Regarding Protection of Privacy Under Title II of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and by FERPA.

6. Will not engage in unauthorized activities. These include, but are not limited to:

   a. Accessing unauthorized information.

b. Knowingly spreading computer viruses.

c. Violating copyright laws (see Policy 1630) or the privacy of others.

d. Plagiarism.

e. Accessing computer systems via another user's account or facilitating unauthorized access by another.

f. Hacking, defacing (including affixing stickers), or destroying school computer systems or disrupting the CCPS network.

g. Circumventing and/or disabling content filtering or other computer system protection measures put in place by the System Administrator, without proper authorization. This includes, but is not limited to, using:

   1) Virtual Private Networks (VPNs). While using VPNs is encouraged to protect people's privacy on personal devices, they are prohibited from being installed on CCPS-issued devices without prior approval from the System Administrator or designee.

   2) Remote control software to access computer systems off the CCPS network

h. Installing or modifying software or hardware on the CCPS computer systems without authorization from the System Administrator or designee, including, but not limited to, moving the computer, changing the configuration of the computer, installing software, and booting an operating system or configuration that has not been approved by the System Administrator or designee.

i. Decrypting passwords and/or gaining unauthorized elevated access or privileges or attempting to do so.

j. Using CCPS computer systems for personal gain or any illegal activities.

k. Accessing, downloading, or installing games or software that have not been approved by CCPS.

l. Installing or copying CCPS software and applications to non-CCPS equipment except as specified by licensing agreements.

m. Removing computer or related equipment from CCPS property without authorization from the System Administrator or designee.

7. 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 the 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 or group or otherwise infringe on the rights of others.

g. 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, cyberbullying, harassment, or intimidation in violation of the Student Code of Conduct and/or CCPS policies and procedures (See Policy 1118 and Procedure 1118.3 regarding discrimination).

8. Are responsible for ensuring all the files they store on CCPS computer systems adhere to the requirements and standards found within these procedures.

9. Will immediately report to the System Administrator portions of the Internet that contain inappropriate material or material that is harmful to students that is not blocked through the content filtering process.

B. The following additional conditions apply to the use of CCPS computer systems by staff (in addition to Part "A" above):

1. Staff are to use CCPS computer systems in a responsible, ethical manner consistent with their professional responsibilities.

2. Staff are responsible for the content of all electronic communication sent from their accounts. Guidelines regarding appropriate email use and content will be made available to all email account holders annually.

3. Staff are prohibited from using CCPS owned equipment to knowingly access or attempt to access portions of the Internet that do not promote the educational, instructional, administrative, business, or support services purposes of CCPS or is not related to any instruction, project, job, work assignment, task, or function for which the user is responsible. Staff may access computer systems for limited amounts of time for personal use when job responsibilities will not be impacted (e.g., lunch, before school, after school). Staff personal use is subject to all user responsibilities and conditions in this procedure.

4. To safeguard against unauthorized disclosure, use, and dissemination of personal identifying information about students, staff will educate students on responsible Internet use. This includes emphasizing personal safety practices such as not sharing personal identifying student information or meeting with anyone they have corresponded with online.

5. Staff members must not disclose student or parent/guardian email addresses to unauthorized individuals or agencies. This prohibition extends to displaying email addresses in the greeting (To:) or carbon-copy (Cc:) fields of an email when sending emails to multiple recipients, Staff members must adhere to

either of the following guidelines when sending emails to more than one outside (non-CCPS) recipient:

   a. Use the blind carbon-copy (Bcc:) box to include multiple recipients, instead of the carbon-copy (Cc:) box.

   b. Send individual emails to each recipient, instead of one email with multiple email addresses in the Cc: and/or To: boxes.

6. Staff assigning directed Internet use by students will prescreen network resources to specify those which are applicable to the curricular needs of the assignment and the developmental level of the student(s). Staff members are responsible for providing appropriate adult supervision and monitoring of learning activities.

7. Staff permitting or assigning use of computer systems by students will ensure that appropriate use of computer technology is occurring. Examples include but are not limited to:

   a. Adhering to the contents of this policy and accompanying procedures.

   b. Adhering to MSDE Health and Safety Best Practice Guidelines (screentime, eye and stretch breaks, etc).

   c. Adhering to Policy and Accompanying Procedures 1630: Use of Copyrighted Materials.

   d. Utilizing approved digital tools.

   e. Utilizing procedures for appropriately accessing and using computer systems and digital tools (logging in, accessing Wi-Fi, etc.).

   f. Promoting Digital Citizenship.

8. Staff assigning students to use an online tool should follow the Student Data Governance and Privacy policy 1925 and accompanying procedures 1925.1 to ensure that the tool has been vetted and approved by CCPS for student data security, privacy, and accessibility.

C. The following apply to the use of CCPS computer systems by students (in addition to Part “A” above):

1. Students may not use the Internet unless they have been provided direction and purpose by their teacher(s).

2. Students may not reveal personally identifiable information (e.g., phone numbers, addresses) 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 and teacher supervision are required.

III. Staff Technology Accounts

A. Access privileges for staff to CCPS computer systems will be granted on an as-needed basis, subject to established guidelines. When staff members 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.

B. Accounts for staff members who are on leave of absence or who are no longer employed by CCPS will be disabled on the 14th calendar day (two weeks) after their last day of employment. The Department of Human Resources is responsible for notifying the System Administrator when employment is terminated so that individual accounts and access privileges can be disabled. Electronic data remains the property of CCPS.

C. All use of CCPS computer systems must be for educational purposes and are subject to review and may be logged and archived. The Superintendent or his/her designee has the right to monitor file server space and review materials on user accounts when a legitimate business need exists or is otherwise necessary to promote the interests of the Calvert County Public Schools. If it becomes necessary for an individual other than the user to access a specific user's email and/or computer system, approval will be obtained from the Superintendent or designee and access will be monitored by the Director of Information Technology.

IV. Employee Personal Websites and Social Media Accounts

A. Material posted on staff members' personal websites and social media sites must model the professional behavior employees are expected to exhibit as a classroom instructor. When creating a personal account, employees need to distinguish between accounts created for professional and personal use.

1. Employees are encouraged to use privacy settings to protect themselves when using social media platforms.

2. Establishing personal online communication with students and parents may compromise professional roles. Employees are encouraged to take care in their communication with parents and avoid such connections with students.

3. Employees must maintain student confidentiality and privacy, refraining from comments on or posts about students online.

4. Employees must adhere to copyright and fair use guidelines when posting or contributing online.

B. Inappropriate content, including messages and pictures, that diminishes an employee's professionalism, discredits his/her capacity to maintain the respect of students and parents, or impairs the ability of the employee to serve as a role model for students is prohibited. CCPS may intervene as noted in the employee handbook.

1. This type of material includes text or pictures involving:

a. Hate speech

b. Bullying

c. Nudity

d. Obscenity

e. Vulgarity

f. Sexually explicit content

g. Discrimination

h. Harassment

i. Other material which creates or may reasonably be expected to create a disruption to the learning environment

V. Employee Professional Websites and Online Learning Platforms

A. Material posted on websites designed by teachers for student use and online learning platforms must model the professional behavior employees are expected to exhibit as a classroom instructor.

B. Inappropriate content, including messages and pictures, that diminishes an employee's professionalism, discredits his/her capacity to maintain the respect of students and parents, or impairs the ability of the employee to serve as a role model for students is prohibited.

C. Utilize safe and secure online learning platforms that have been vetted and approved by CCPS.

D. When working directly with students virtually, staff will use the Microsoft Teams application.

E. Obtain parental permission before students under the age of 13 create content or posts using accounts with personally identifiable information such as an email address.

VI. Department/School Professional Social Media Accounts

A. The term "social media" describes the online technologies available for people to share information, opinions, experiences, and perspectives with each other. "Social Media" may be defined as any on-line technologies where people share information, opinions, experiences, and perspectives. Examples include, but are not limited to, X (formerly Twitter), Facebook, YouTube, Instagram, and Snapchat. It also includes all electronic communications, including, but not limited to, texting, emailing, instant messaging, group messaging, and chat rooms. Many more social media applications exist, and new platforms are being created all the time.

B. These applications are subject to the same policies and approvals as any other application used for official CCPS business. Individuals interested in creating an official CCPS social media account should work with the Webmaster and/or the Supervisor of Application Technologies to discuss the process.

C. Employees may initiate, monitor, or update social media relating to CCPS if their principal or department supervisor has assigned or approved their doing so. Before granting such approval, principals and department directors should consider the fact that social media may become public records if used to conduct CCPS business. This is subject to records retention and disclosure requirements. Additionally, CCPS may be responsible for the content of such records and for monitoring or maintaining any relevant applications, as well as supervising employees working on social media sites.

D. The naming of a social media site or page should be created using the following naming convention: Department or school, group, Calvert County Public Schools. For example: "Calvert High School, Calvert County Public Schools" or "Student Services, Calvert

County Public Schools" or "Calvert High, Counseling Department, Calvert County Public Schools."

E. Avoid using an individual CCPS employee's email address when registering for a social media website pertaining to CCPS. Generic school or department emails should be used to ensure site access in the event responsibilities shift to another employee. IT will provide a generic email to set up social media accounts for schools and departments.

F. Sites with comments, questions, and response capability should include the following disclaimer: *Posts and other content added by curators of the [insert name of social media platform] pages of Calvert County Public Schools are official Calvert County Public Schools information. Comments and opinions expressed by other non-CCPS users, and links to non-CCPS sites, do not necessarily reflect the opinion of Calvert County Public Schools.*

   By providing the opportunity to post, [insert name of program or school] is providing only a limited open forum. Excluded topics are material unrelated to the announced topic, employee personnel information, individually identifiable student information, copyrighted material without permission, confidential material, or obscene, defamatory, discriminatory, violent, threatening, vulgar, or sexual material, or material that will create a substantial disruption to the school(s). Calvert County Public Schools reserves the right to remove content that does not comply with these guidelines or that otherwise may create a substantial disruption in the school or workplace. It will not, however, discriminate on the basis of viewpoint. Unauthorized advertising, business solicitations, spam, sales, other commercial messages, political or campaign messages, and other personal expression unrelated to the topic or for pages dealing with all aspects of CCPS, the mission and operation of the schools, also will be removed. Users are encouraged to report content that violates [inset name of social media platform] code of conduct to the CCPS employee listed on this page.

G. Any employee professional use of social media should be public and transparent, and not be intended to be used for one-to-one communication with users, especially students. This includes but is not limited to one-to-one email, messaging, and texting. Schools should not require students to participate in any social media as the sole form of communication/engagement.

H. Employee professional sites should relate to the mission and goals of CCPS, not reflect the staff member's personal views.

I. Always protect student information that is considered identifiable. When posting student photos or videos, be sure that each student's parents/guardians have not opted out for their child's information to be published. Opt-out requests are updated annually and are maintained by the school in the district Student Information System.

VII. Noncompliance

A. Any suspected violation of Policy 2718 and/or these procedures should be reported to the appropriate administrator or supervisor for investigation and possible discipline in accordance with CCPS policies and procedures including the Student Discipline Policy 1112 and Employee Discipline Policy 1750.