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 Communication Media

I. Definitions

A. The Calvert County Public Schools (CCPS) Web – all publicly accessible Web content for district, school, and department pages.

B. Computer Systems – all hardware, software, and related technology including wired and wireless networks, and communications equipment such as mobile devices and portable computers.

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

D. Educational 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 that the user is responsible.

E. Electronic Communication Media – this includes any media used to communicate electronically, including computers, mobile devices, the Internet, and websites, whether the media is owned, leased, or not owned by CCPS.

F. Electronic Data – facts and information contained in any electronic form including but not limited to files, records, and e-mail.

G. E-mail – a means or system for transmitting messages electronically; messages sent and received electronically through such means or system.

H. Hate Speech – speech that attacks a person or group on the basis of race, ethnicity, religion, gender, or sexual orientation, or any other association or personal characteristics including bullying and cyberbullying.

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 material interference with school activities and/or the school's learning environment.

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

K. Social Media- Websites and application used for social networking.

L. Social Networking - A platform to build social relations among people who share interests, activities, backgrounds or real-life connections.

M. Staff - all employees and temporary employees of the Calvert County Public Schools.

N. System Administrator - the Superintendent's designee responsible for implementing and maintaining the school system's hardware and software infrastructure; enforcing related policies, including internal and external access and security; and managing service technicians.

O. User - any CCPS staff member, student, or other individual authorized to use the CCPS computer systems. Other individuals may include parents, volunteers, and contract or temporary staff

P. Web Services – the unit responsible for managing the CCPS Web, under the direction of the Director of Information Technology. The webmaster is the site manager for the CCPS Web.

II. User Responsibilities

A. Users of CCPS computer systems and employees when engaging in school system business:

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 an ethical, efficient, responsible, and legal manner.

3. 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.

4. With the exception of 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

    a. Procedures 1920: Regarding Records Retention and Disposal, Policy and

    b. Procedure Regarding Protection of Privacy Under Title II of the Health

    c. Insurance Portability and Accountability Act of 1996 (HIPAA) and by FERPA.

5. 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. Entering (hacking) into, destroying (including physically destructing) school computer systems, or disrupting the network.

g. Circumventing and/or disabling content filtering or other computer system protection measures put in place by the System Administrator, without proper authorization.

h. Installing 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.

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

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

6. Will not install or copy CCPS software and applications to non-CCPS equipment except as specified by licensing agreements.

7. Are responsible for their files stored on CCPS computer systems.

8. Will not remove computer or related equipment from CCPS property without authorization by the System Administrator.

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

B. The following additional conditions apply to the use of CCPS computer systems by staff:

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. A standard confidentiality notice provided by the System Administrator will be attached to the bottom of all e-mail sent through the CCPS e-mail system. Guidelines regarding appropriate email use and content will be made available to all email account holders.

3. Users 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 (i.e. lunch, before school, after school). Staff personal use is subject to all user responsibilities and conditions in this procedure.

4. In order to prevent the unauthorized disclosure, use and dissemination of personal identifying information regarding students, staff will work to educate students on appropriate use of the Internet, particularly personal safety practices including, but not limited to, release of personal identifying student

information and meetings with anyone with whom a student corresponded online.

5. Staff members shall not reveal student or parent/guardian email addresses to any unauthorized (non –CCPS) individual or agency. This includes making the email addresses visible in the email greeting (To:) or carbon-copy (CC:) boxes of an email. When sending emails to multiple recipients, CCPS users must take precautions to ensure that each outside (non-CCPS) recipient's email address remains hidden from the other parties on that email. 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 in order 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 instruction in acceptable use of computer technology has occurred. Topics to be taught include:
    a. The contents of this policy and accompanying procedures.
    b. Procedures for appropriately accessing computer systems (logging in, accessing network resources, etc.).
    c. Procedures for using specific Internet tools.
    d. Provisions contained in the school system Internet permission forms.
    e. Safety guidelines.
    f. Evaluating types of information sources and assessing the appropriateness of using the Internet as a resource for a specific learning activity.
    g. Copyright and privacy issues.
8. Web tools and sites which support collaborative discussions (i.e. Wikis, blogs, instant messaging, threaded discussions, social networking sites, etc.) should be used with caution. Staff members that use these tools/sites must complete a CCPS developed training module and are responsible for closely monitoring discussions, posted content, and student interactions for appropriateness of content, educational purposes and confidentiality.

C. The following apply to the use of CCPS computer systems by students:
    1. Students are responsible for their behavior on school computer systems.

2. Students may not go online unless they have been provided direction and purpose by their teacher(s), including a review of the school rules related to computer systems and online etiquette.
3. Students may not reveal personally identifiable information (e.g., home 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.
4. Students will access only those network resources for which they have obtained permission, using only the account assigned to them.
5. Students 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 person or group or otherwise infringe on the rights of others.
    g. Cause or are likely to 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, cyber-bullying, 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.)
6. Students may not access, download, or install online games without the permission of a school administrator.

III. Staff Technology Accounts

A. Access privileges for staff to CCPS computer systems will be granted on an as needed basis and 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 day 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 as 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 e-mail 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 Other Social Media Accounts

A. Material posted on staff members' personal websites and other social networking 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 in order 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, which diminishes an employee's professionalism or discredits his/her capacity to maintain the respect of students and parents, or that will impair the ability of that employee to serve as a role model for students is prohibited.

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 and/or
    g. Other material which creates or may reasonably be expected to create a disruption to the learning environment.
    h. Discrimination
    i. Harassment

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, which diminishes an employee's professionalism or discredits his/her capacity to maintain the respect of students and parents, or that will impair the ability of that employee to serve as a role model for students is prohibited.

C. Utilize safe and secure education portals whenever available.

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

VI. 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