PERSONNEL: Conduct

[Technology] Acceptable Use Policy FOR TECHNOLOGY AND SOCIAL MEDIA (TAUP) for Authorized Users

I. Purpose

To implement Board of Education of Baltimore County (Board) Policy 4104 by establishing guidelines for the use of technology and social media by authorized users in Baltimore County Public Schools (BCPS) and by outlining appropriate use and prohibited activities when using BCPS technology AND SOCIAL MEDIA.

II. Definitions

A. **Authorized User** – Any employee, Board member or approved non-employee who has been authorized by the school principal or office head to have access to BCPS technology to carry out his/her duties for the school system.

B. **Crowdfunding** – The practice of funding a project or venture by raising many small amounts of money from a large number of people, typically via the Internet.

C. **Educational Purposes** – Those tasks performed by employees and approved non-employees for legitimate educational, school-related, administrative or business purposes related to the operation of BCPS.

D. **Employee** – Persons employed by the school system on a regular and/or temporary basis.

E. **Internet** – A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.

F. **Network** – The system of devices, kiosks, servers, databases, routers, hubs, switches and distance learning equipment.

G. **Non-Employee** – AN INDIVIDUAL WHO UTILIZES BCPS TECHNOLOGY BUT WHO IS NOT AN EMPLOYEE OF THE SCHOOL SYSTEM (E.G., volunteer, intern, SCHOOL RESOURCE OFFICER, independent contractor or an individual working for BCPS under a consultant
agreement or purchase order and paid through the Department of Fiscal Services).

G. *PERSONAL SOCIAL MEDIA* – A NON-WORK-RELATED SOCIAL MEDIA ACTIVITY FOR AN INDIVIDUAL’S OWN PERSONAL USE.

H. *PROFESSIONAL SOCIAL MEDIA* - A BCPS WORK-RELATED SOCIAL MEDIA ACTIVITY (E.G., A PRINCIPAL ESTABLISHING A FACEBOOK PAGE FOR THEIR OWN SCHOOL, OR A TEACHER ESTABLISHING A BLOG FOR THEIR CLASS OR AN ADMINISTRATIVE OFFICE’S TWITTER ACCOUNT ABOUT SCHOOL SYSTEM ACTIVITIES).

I. [H.] *Social Media* – ANY FORM OF ELECTRONIC COMMUNICATION THROUGH WHICH USERS COMMUNICATE INTERACTIVELY. SOCIAL MEDIA INCLUDE, BUT ARE NOT LIMITED TO, BLOGS AND MICROBLOGS (LIKE TWITTER), APPLICATION SOFTWARE (LIKE INSTAGRAM), AND SOCIAL NETWORKING WEBSITES (LIKE FACEBOOK). [Any form of online publication or presence that allows interactive communication including, but not limited to, social networks, blogs, Internet Web sites, Internet forums and Wikis. Examples of social media include, but are not limited to, Facebook™, Twitter™, YouTube, Google+, Instagram, Snapchat and LinkedIn.]

J. [I.] *Technology* – ANY SYSTEMS, SOFTWARE OR HARDWARE USED BY AUTHORIZED USERS [Any electronic device or system] that uses, stores, manages, carries[,] or supports audio, video, text or data [and includes, but is not limited to, information transmitted or received via radio, television, cable, microwave, telephone, computer systems, networks, copiers, scanners, cell phones/smart devices and fax machines].

K. [J.] *Webmaster* – An EMPLOYEE [authorized user] who is responsible for the content and publication of a school OR [/]office Web site.

III. ACCEPTABLE USE GUIDELINES

THE FOLLOWING GUIDELINES SHALL BE FOLLOWED WHEN USING BCPS TECHNOLOGY AND PROFESSIONAL SOCIAL MEDIA.
A. ALL TECHNOLOGY OWNED AND/OR LEASED BY BCPS ARE TO BE CONSIDERED THE DOMAIN OF BCPS AND ARE SUBJECT TO THE REQUIREMENTS OF THIS RULE.

B. ALL COMMUNICATIONS TRANSMITTED BY BCPS TECHNOLOGY AND PROFESSIONAL SOCIAL MEDIA SHALL BE PROFESSIONAL AND RESPECTFUL IN TONE AND CONTENT. AUTHORIZED USERS SHALL USE BCPS TECHNOLOGY AND PROFESSIONAL SOCIAL MEDIA IN A RESPONSIBLE, CIVIL, ETHICAL AND LEGAL MANNER.

C. AUTHORIZED USERS SHALL:
   1. COMPLY WITH PRIVACY RIGHTS OF ALL PERSONS;
   2. COMPLY WITH COPYRIGHT LAWS AND INTELLECTUAL PROPERTY RIGHTS OF OTHERS;
   3. IMMEDIATELY REPORT TO THE USER’S IMMEDIATE SUPERVISOR, OR TO THE DEPARTMENT OF INFORMATION TECHNOLOGY IF THE SUPERVISOR IS NOT AVAILABLE, THE RECEIPT OF ELECTRONIC MESSAGES, WHICH THREATEN TO ENDANGER THE SAFETY OF STUDENTS, EMPLOYEES OR OTHER PERSONS;
   4. SAFEGUARD CONFIDENTIAL INFORMATION MADE AVAILABLE TO THEM. ANY WRONGFUL DISCLOSURE OF PERSONAL/CONFIDENTIAL INFORMATION SHALL BE REPORTED IMMEDIATELY TO THE USER’S SUPERVISOR. NOTICE OF THE BREACH SHALL BE MADE IN ACCORDANCE WITH THE MARYLAND PERSONAL INFORMATION PROTECTION ACT.

D. AUTHORIZED USERS SHALL NOT ENGAGE IN PROHIBITED ACTIVITIES, INCLUDING, BUT NOT LIMITED TO, THE FOLLOWING:
   1. BYPASSING THE SCHOOL SYSTEM’S WEB CONTENT FILTER;
   2. ACCESSING, UPLOADING, DOWNLOADING, DISTRIBUTING, OR COMMUNICATING PORNOGRAPHIC OR SEXUALLY EXPLICIT IMAGES, OR USING LANGUAGE OR THE FILES WHICH GENERATE SUCH IMAGES;
   3. CREATING OR COMMUNICATING ABUSIVE, HARASSING, BULLYING, LIBELOUS, OBSCENE, OFFENSIVE, PROFANE, THREATENING, DISCRIMINATORY OR ILLEGAL
COMMUNICATIONS OR USING ANY LANGUAGE OR SYMBOLS THAT PROMOTE HATE, RACIAL OR ETHNIC VIOLENCE OR INTIMIDATION;

4. USING TECHNOLOGY FOR ANY ILLEGAL ACTIVITY OR FOR PERSONAL GAIN OR PROFIT, LOBBYING OR ANY PERSONAL BUSINESS OR COMMERCIAL ACTIVITY;

5. KNOWINGLY ENTERING UNAUTHORIZED COMPUTER NETWORKS OR SOFTWARE TO TAMPER OR DESTROY DATA OR PERFORMING NETWORK SCANNING ACTIVITIES UNLESS AUTHORIZED BY THE NETWORK SUPPORT SERVICES TEAM;

6. INSTALLING UNAUTHORIZED SOFTWARE OR HARDWARE ON BCPS TECHNOLOGY;

7. INCURRING UNAUTHORIZED FINANCIAL OBLIGATIONS ON BEHALF OF BCPS;

8. SHARING USERNAME AND/OR PASSWORDS TO ACCESS BCPS TECHNOLOGY;

9. KNOWINGLY UPLOADING OR COMMUNICATING ELECTRONIC FILES (SUCH AS VIRUSES), WHICH WOULD HAVE THE EFFECT OF VANDALIZING, DAMAGING OR DISABLING BCPS TECHNOLOGY EQUIPMENT OR SYSTEMS; AND

10. ACCESSING ANOTHER INDIVIDUAL’S MATERIALS, INFORMATION OR FILES WITHOUT AUTHORITY.

E. AUTHORIZED USERS ARE RESPONSIBLE FOR ALL ACTIVITY ORIGINATING FROM THEIR ACCOUNTS.

F. WHEN USING BCPS TECHNOLOGY FOR CLASS ACTIVITIES, SCHOOL AND ADMINISTRATIVE STAFF WILL MODEL THE APPROPRIATE, LEGAL, ETHICAL AND SAFE USE OF TECHNOLOGY.

G. BCPS TECHNOLOGY SHALL BE USED CONSISTENT WITH EMPLOYEE JOB RESPONSIBILITIES AND INSTRUCTIONAL REQUIREMENTS.

A. EMPLOYEES
1. EMPLOYEES WILL BE PROVIDED WITH A COPY OF BOARD POLICY AND SUPERINTENDENT’S RULE 4104, ACCEPTABLE USE POLICY FOR TECHNOLOGY AND SOCIAL MEDIA (TAUP) FOR AUTHORIZED USERS AS PART OF THE BCPS ONBOARDING PROCESS.

2. EMPLOYEES WILL BE REQUIRED TO SIGN THE TECHNOLOGY AND SOCIAL MEDIA ACCEPTABLE USE AGREEMENT (RULE 4104, FORM A), INDICATING THAT THEY HAVE READ, UNDERSTOOD AND AGREED TO ABIDE BY THE ACCEPTABLE USE POLICY AND THIS RULE BEFORE RECEIVING ACCESS TO BCPS TECHNOLOGY.

3. EMPLOYEES WILL BE PROVIDED ACCESS TO AND PERMISSION TO USE BCPS TECHNOLOGY IN ALIGNMENT WITH THEIR JOB RESPONSIBILITIES.

4. THE SIGNED TECHNOLOGY AND SOCIAL MEDIA ACCEPTABLE USE AGREEMENT SHALL BE MAINTAINED IN THE EMPLOYEE’S OFFICIAL PERSONNEL FILE IN THE DIVISION OF HUMAN RESOURCES.

B. NON-EMPLOYEES
1. [A.] Principals or office heads are responsible for determining when [employees and] non-employees will have access to, and privileges on, BCPS technology. [The principal or office head will identify authorized users and determine which level(s) of access is required for the users to perform their assigned duties.]

2. [B.] NON-EMPLOYEES [Authorized users] will be provided with a copy of BOARD Policy AND SUPERINTENDENT’S RULE 4104 [4101], [Technology] Acceptable Use Policy FOR TECHNOLOGY AND SOCIAL MEDIA (TAUP) for Authorized Users [and this Rule] and will be required to sign the TECHNOLOGY AND SOCIAL MEDIA ACCEPTABLE USE AGREEMENT (RULE 4104, FORM A), INDICATING THAT THEY HAVE READ, UNDERSTOOD AND AGREED TO ABIDE BY THE ACCEPTABLE USE POLICY AND THIS RULE BEFORE RECEIVING ACCESS TO BCPS TECHNOLOGY [forms for each authorized level of access prior to using or connecting to BCPS technology and the Internet]. NON-EMPLOYEES WILL BE REQUIRED TO SIGN THE
TECHNOLOGY AND SOCIAL MEDIA ACCEPTABLE USE AGREEMENT AT THE BEGINNING OF EACH SCHOOL YEAR.

3. THE APPROVING PRINCIPAL OR OFFICE HEAD SHALL MAINTAIN THE SIGNED ACCEPTABLE USE AGREEMENT FOR ALL NON-EMPLOYEES IN THEIR OFFICE FILES AND MAINTAIN THE ACCEPTABLE USE AGREEMENTS AS REQUIRED BY THE APPLICABLE RECORDS RETENTION SCHEDULE.

[C. Required Forms

1. Level 1: Internet
   a. Prior to using BCPS Technology or connecting to the Internet, authorized users are required to sign the Acceptable Use Agreement for Authorized Users (See, Rule 4104, Form A).
      (1) The signed acceptable use agreement shall be maintained as follows:
         (a) Employees – In the employee’s official personnel file in the Division of Human Resources.
         (b) Independent contractors – By the Department of Information Technology.
         (c) Volunteers/interns – With the approving principal or office head.

2. Level 2: E-Mail
   a. Prior to establishing an e-mail account, authorized users are required to sign the BCPS Electronic Mail Application Form (See, Rule 4104, Form C).
      (1) The signed e-mail application forms shall be maintained as follows:
         (a) Employees – In the employee’s official personnel file (paper or electronic) in the Division of Human Resources.
         (b) Non-Employees – By the Department of Information Technology.
   b. Authorized users are required to notify the Department of Information Technology of any changes in legal name, employment status, work location or position change by submitting an Electronic Mail Change Form (See, Rule 4104, Form D).

3. Level 3: Web Posting/Publishing
a. School and office Webmasters are required to sign the BCPS Webmaster Agreement Form (See, Rule 4104, Form B).
   (1) Persons authorized under this subparagraph are required to attend annual training.
   (2) The Department of Information Technology shall retain all signed Webmaster forms.

[IV. Guidelines]

A. All computer hardware, software, electronic files, peripheral devices and technology owned and leased by BCPS are to be considered the domain of BCPS and are subject to the requirements of this rule.

B. Authorized users are responsible for any activity originating from their accounts.

C. All BCPS technology shall be used for educational purposes and/or for fulfilling the professional job requirements of authorized users. Use of BCPS technology or networks for any illegal activity is prohibited.

D. Authorized users of BCPS computers, networks, services and/or information resources may not disclose their password to anyone.

E. Access to BCPS technology may be terminated at any time as determined by the Department of Information Technology, without notice.

[V. Instructional Responsibilities]

A. When using BCPS technology and digital content for class activities, school and administrative staff will instruct students in the appropriate, legal, ethical and safe use of technology.

B. School staff will monitor and supervise all student use of BCPS technologies.

C. BCPS-generated student passwords shall be used when creating accounts for students on authorized web-based resources.]


V. SCHOOL SYSTEM WEB SITES

A. THE WEBMASTER IS RESPONSIBLE FOR THE CONTENT AND PUBLICATION OF A BCPS SCHOOL/OFFICE WEB SITE.

B. THE WEBMASTER SHALL ADHERE TO THE FOLLOWING REQUIREMENTS:
   1. USING THE BCPS WEB CONTENT MANAGEMENT SYSTEM (CMS) TEMPLATES TO CREATE AND POST SCHOOL/OFFICE WEB PAGES AND CONTENT;
   2. FOLLOWING INTERNAL DEPARTMENT OF INFORMATION TECHNOLOGY PROCEDURES FOR APPROVAL BY SCHOOL/OFFICE HEAD PRIOR TO POSTING WEB PAGES AND CONTENT;
   3. MAINTAINING THE SCHOOL/OFFICE WEB SITE AND CONTENT FOR ACCURACY, ACCESSIBILITY, RELEVANCE AND APPROPRIATENESS;
   4. RESPONDING TO COMMUNICATIONS RELATED TO ACCESSING THE WEB PAGES AND CONTENT;
   5. COMPLYING WITH STUDENT PRIVACY OPTIONS PRIOR TO PUBLISHING CONTENT, INCLUDING DIRECTORY INFORMATION;
   6. ATTENDING ALL REQUIRED TRAININGS; AND
   7. FOLLOWING ESTABLISHED SCHOOL/OFFICE WEB SITE GUIDELINES PROVIDED BY BCPS’ DEPARTMENT OF COMMUNICATIONS AND COMMUNITY OUTREACH.

C. NO BCPS WEB SITE SHALL INCLUDE ADVERTISEMENTS OR IMPLY ENDORSEMENT OF BUSINESSES OR PRODUCTS.

D. BCPS WEB SITES SHALL CONTAIN, OR LINK TO, THE A WEB ACCESSIBILITY NOTICE AND THE FOLLOWING DISCLAIMER:

   BALTIMORE COUNTY PUBLIC SCHOOLS (BCPS) MAKES EVERY REASONABLE ATTEMPT TO ENSURE THAT OUR SCHOOL SYSTEM’S WEB SITES ARE EDUCATIONALLY SOUND AND DO NOT CONTAIN LINKS TO ANY CONTENT THAT CAN BE DEEMED IN VIOLATION OF THE BCPS TECHNOLOGY ACCEPTABLE USE POLICY. LINKED SITES ARE NOT UNDER THE CONTROL OF BCPS BUT ARE PROVIDED AS A CONVENIENCE AND DO NOT
IMPLY AN ENDORSEMENT OF THE LINKED WEB SITE OR ITS CONTENTS. BCPS IS NOT RESPONSIBLE FOR WEB CONTENT ACCESSIBILITY OF LINKED SITES.

VI. PROFESSIONAL Social Media

AS PROVIDED IN POLICY 4104, THE BOARD SUPPORTS THE USE OF PROFESSIONAL SOCIAL MEDIA SITES TO PROMOTE THE EDUCATIONAL MISSION OF BCPS. EMPLOYEES SHALL ADHERE TO THE ACCEPTABLE USE GUIDELINES AS WELL AS THE FOLLOWING REQUIREMENTS WHEN USING PROFESSIONAL SOCIAL MEDIA.

A. PROFESSIONAL SOCIAL MEDIA SITES MAY BE USED TO FACILITATE COMMUNICATION AMONG EMPLOYEES, GROUPS OF STUDENTS TO FURTHER THE INSTRUCTIONAL PROGRAM AND TO COMMUNICATE WITH THE SCHOOL COMMUNITY. BCPS PROFESSIONAL SOCIAL MEDIA ACCOUNTS ARE THE PROPERTY OF BCPS. [Employees are required to use social media sites solely for BCPS’ educational purposes, whether in connection with lessons and assignments or to facilitate communication within BCPS and the community.]

B. PRIOR TO CREATING A BCPS-RELATED PROFESSIONAL SOCIAL MEDIA ACCOUNT, EMPLOYEES MUST OBTAIN THEIR PRINCIPAL’S OR OFFICE HEAD’S WRITTEN APPROVAL.

C. THE PRINCIPAL OR OFFICE HEAD IS RESPONSIBLE FOR MAINTAINING A LIST OF ALL PROFESSIONAL SOCIAL MEDIA ACCOUNTS WITHIN THEIR SCHOOL OR OFFICE. IF THE EMPLOYEE’S JOB RESPONSIBILITIES CHANGE OR EMPLOYMENT ENDS, THE PRINCIPAL OR OFFICE HEAD WILL RESET ADMINISTRATIVE ACCESS TO THE PROFESSIONAL SOCIAL MEDIA ACCOUNT TO WHICH THE EMPLOYEE HAD ACCESS.

D. PROFESSIONAL SOCIAL MEDIA ACCOUNTS SHALL BE LINKED TO BCPS E-MAIL ACCOUNTS ONLY AND REMAIN SEPARATE FROM ANY PERSONAL SOCIAL MEDIA ACCOUNTS.

E. [B.]Employees are prohibited from utilizing their personal social media accounts and/or Web sites for official school purposes.
F. [C.] Any student information communicated through professional social media platforms must comply with all school system policies, rules and procedures on student privacy, including Board Policy and Superintendent’s Rule 5230, *Student Records*, and Board Policy and Superintendent’s Rule 6202, *Technology Acceptable Use Policy (TAUP) for Students*.

G. EMPLOYEES [Teachers] are required to comply with parental privacy options for the release of a student’s directory information AND FOR THE PUBLICATION OF A STUDENT’S INTELLECTUAL PROPERTY AND/OR STUDENT-CREATED PUBLICATIONS WHEN POSTING TO A PROFESSIONAL SOCIAL MEDIA SITE [through social media platforms].

[D. Wherever possible, teachers are encouraged to use school-system owned and controlled collaborative content sites in BCPS One.

1. A teacher is required to obtain approval from his/her principal prior to using any non-BCPS operated/controlled social media within the classroom or for educational purposes.

2. Non-BCPS operated/controlled social media platforms may only be approved by the school principal when the educational benefit outweighs the potential risks, the students using the platform are properly educated regarding online safety and no other unbounded or BCPS operated/controlled platform would be able to achieve the same purpose.

3. The principal or his/her designated administrator is responsible for maintaining a list of all professional social media accounts within his/her school.]

H. [E.] Professional social media communication must comply with existing Board policies, Superintendent’s rules, school system procedures and applicable laws, including, but not limited to, prohibitions on the disclosure of confidential information and prohibitions on the use of harassing, obscene, discriminatory, defamatory or threatening language.

[F. Employees shall comply with the school system’s social media guidelines.]
VII. PERSONAL USE OF SOCIAL MEDIA

BCPS RECOGNIZES THAT EMPLOYEES MAY ALSO HAVE A PERSONAL PRESENCE ON SOCIAL MEDIA SITES. EMPLOYEES SHOULD BE AWARE THAT THEY MAY BE IDENTIFIED AS A SCHOOL SYSTEM EMPLOYEE. BCPS ENCOURAGES EMPLOYEES WHO HAVE SUCH PRESENCE TO CONTINUE TO ADHERE TO BOARD POLICIES AND SUPERINTENDENT’S RULES IN THEIR PERSONAL USE OF SITES. EMPLOYEE’S WILL FOLLOW THESE GUIDELINES ON PERSONAL SOCIAL MEDIA SITES.

A. EMPLOYEES ARE PROHIBITED FROM UTILIZING THEIR PERSONAL SOCIAL MEDIA ACCOUNTS AND/OR WEB SITES FOR OFFICIAL SCHOOL PURPOSES.

B. EMPLOYEES MAY NOT USE THEIR PERSONAL SOCIAL MEDIA PRESENCE TO COMMUNICATE IMPROPER OR INAPPROPRIATE MESSAGES OR CONTENT WITH OR ABOUT BCPS STUDENTS OR EMPLOYEES.

C. EMPLOYEES MAY NOT DISCLOSE STUDENT OR EMPLOYEE RECORDS OR PERSONAL OR CONFIDENTIAL INFORMATION REGARDING STUDENTS OR EMPLOYEES USING THEIR PERSONAL SOCIAL MEDIA.

D. EMPLOYEES MAY NOT POST IMAGES OF ANY BCPS STUDENT TO ANY PERSONAL SOCIAL MEDIA SITE FOR ANY REASON, UNLESS THE STUDENT IS A RELATIVE OF THE EMPLOYEE AND THE EMPLOYEE HAS RECEIVED WRITTEN PERMISSION TO POST THE IMAGE OF THE STUDENT FROM THE STUDENT’S PARENT OR GUARDIAN.

VIII. [VII.] Crowdfunding GUIDELINES

A. Employees WHO wish[ing] to raise funds for a particular school or classroom by use of donation-based crowdfunding PLATFORM shall obtain the written approval of their principal prior to posting any mention of a particular school or the school system on a crowdfunding site.

B. THE PRINCIPAL SHALL SEEK THE APPROVAL OF THE DEPARTMENT OF INFORMATION TECHNOLOGY PRIOR TO AUTHORIZING ANY CROWDFUNDING ACTIVITY THAT
INVOLVES THE PURCHASE OF OR DONATION OF TECHNOLOGY, SOFTWARE OR WEB-BASED SUBSCRIPTION PURCHASES.

C. CROWDFUNDING ACTIVITIES SHALL ADHERE TO THE FOLLOWING GUIDELINES:

1. ALL CROWDFUNDING ACTIVITIES SHALL COMPLY WITH THE BOARD’S ETHICS CODE POLICIES.

2. ALL CROWDFUNDING ACTIVITIES SHALL BE IN THE NAME OF THE SCHOOL AND NOT AN INDIVIDUAL BCPS EMPLOYEE.

3. THE DISCLOSURE OF STUDENT INFORMATION TO ANY CROWDFUNDING PLATFORM IS STRICTLY PROHIBITED.

4. BCPS PROHIBITS THE POSTING OF STUDENT IMAGES ON ANY CROWDFUNDING SITE. POSTINGS SHALL NOT IDENTIFY STUDENTS BY INTELLECTUAL LEVEL OR ATTAINMENT, SUCH AS “MS. JONES’ SPECIAL EDUCATION OR GIFTED AND TALENTED (G/T) CLASS.”

5. NO SCHOOL BANKING INFORMATION SHALL BE PROVIDED TO ANY THIRD-PARTY CROWDFUNDING PLATFORM.

6. AUTOMATED CLEARING HOUSE (ACH) TRANSFER TRANSACTIONS FOR CROWDFUNDING ACTIVITIES ARE PROHIBITED.

7. MONETARY DONATIONS FROM THE CROWDFUNDING PLATFORM SHALL BE IN THE FORM OF CASH OR CHECK MADE PAYABLE TO THE INDIVIDUAL SCHOOL AND DEPOSITED IN THE SCHOOL’S ACTIVITY FUND ACCOUNT. EMPLOYEES ARE PROHIBITED FROM DEPOSITING FUNDS DIRECTLY INTO THEIR PERSONAL BANK ACCOUNTS.

8. DONATIONS OF SUPPLIES AND MATERIALS SHALL BE DELIVERED DIRECTLY TO THE SCHOOL AND RECEIVED BY THE PRINCIPAL OR ACCOUNT MANAGER. EMPLOYEES ARE PROHIBITED FROM HAVING SUPPLIES AND MATERIALS DELIVERED DIRECTLY TO THE EMPLOYEE’S HOME.

D. [B.] ALL APPROVED CROWDFUNDING ACTIVITIES MUST COMPLY WITH ALL APPLICABLE LAWS, BOARD POLICIES, SUPERINTENDENT’S RULES AND [Employees shall comply] with fundraising procedures established by the Department of Fiscal Services.
E. **ALL MONETARY AND NON-MONETARY ITEMS RECEIVED THROUGH CROWDFUNDING ACTIVITIES ARE THE PROPERTY OF BCPS.**

[C. **BCPS prohibits the posting of student images on any crowdfunding site. Postings shall not identify students by intellectual level or attainment, such as “Ms. Jones’ special education or gifted and talented (G/T) class.”**]

[VIII. Acceptable Use of Technology and Social media]

A. All communications transmitted by BCPS technology shall be professional and respectful in tone and content. Authorized users shall use BCPS technology and social media in a responsible, civil, ethical and legal manner.

B. Authorized Users shall:
1. Comply with privacy rights of all persons;
2. Comply with copyright laws and intellectual property rights of others;
3. Comply with all Board policies, Superintendent’s rules and school system procedures;
4. Immediately report to the user’s immediate supervisor, or to the Department of Information Technology if the supervisor is not available, the receipt of electronic messages, which threaten to endanger the safety of students, employees or other persons;
5. Report suspected violations of the technology acceptable use policy to the user’s immediate supervisor; and
6. Safeguard confidential information made available to them. Any wrongful disclosure of personal/confidential information shall be reported immediately to the user’s supervisor. Notice of the breach shall be made in accordance with the Maryland Personal Information Protection Act.

C. Authorized users shall not engage in prohibited activities, including, but not limited to, the following:
3. Bypass the school system’s Web content filter;
4. Access, upload, download, distribute, or communicate pornographic or sexually-explicit images, language or the files which generate such images or language;
5. Create or communicate abusive, harassing, bullying, libelous, obscene, offensive, profane, threatening, discriminatory or illegal communications;
6. Use technology for personal gain or profit, lobbying, commercial or illegal purposes;
7. Knowingly enter unauthorized computer networks or software to tamper or destroy data or perform network scanning activities unless authorized by the Network Support Services team;
6. Install unauthorized software or hardware on BCPS technology; incur unauthorized financial obligations on behalf of BCPS;
7. Share username and/or passwords to access BCPS technology;
8. Knowingly upload or communicate electronic files (such as viruses), which would have the effect of vandalizing, damaging or disabling BCPS technology equipment or systems; and
9. Access another individual’s materials, information or files without authority.

X. [IX.] Privacy

A. The privacy of communications, data and files on BCPS technology is neither expressed nor implied. The Department of Information Technology may monitor, audit and review data, files and communications to maintain system integrity and to ensure that authorized users are using the system in accordance with Board policies, Superintendent’s rules, school system procedures and applicable federal and state laws.

B. Information transmitted and maintained on BCPS technology is subject to federal and state laws, including the Maryland Public Information Act and the federal Family Educational Rights and Privacy Act. Authorized users are responsible for maintaining data to which they have access or control in accordance with all applicable federal and state laws and regulations.

C. Under the Maryland Public Information Act, written communications, including those transmitted by using BCPS technology AND PROFESSIONAL SOCIAL MEDIA ACCOUNTS [that deal with school system business], may be subject to disclosure. Requests for public records will be processed in accordance with Superintendent’s Rule 2373, Public Information Act Requests.


A. BCPS reserves the right to exercise editorial control over:
1. All electronic publications and communications on all BCPS technology AND SOCIAL MEDIA ACCOUNTS; and
2. All user accounts by setting limits on a user’s file size, storage space and by removing files if the user fails to maintain assigned storage space properly.

B. BCPS electronic communications will be maintained in accordance with the school system’s [electronically stored information (ESI) procedures and in accordance] with the school system’s RECORDS MANAGEMENT PROGRAM [record retention schedule].

C. BCPS will not be responsible for any information that may be lost, damaged or unavailable due to technical or other difficulties.

D. All data and intellectual property created in the performance of duties with BCPS is the property of the Board. All data stored on computers owned by BCPS becomes the property of the Board whether created in performance of duties or not.

[XI. School System Web Sites]

A. The Department of Information Technology shall manage the school system’s Web development.

B. BCPS makes every reasonable attempt to ensure that the school system’s Web sites are educationally sound and do not contain links to any questionable material or material that can be deemed a violation of the BCPS technology acceptable use policy.

C. All school or system-level Web sites shall contain, or link to, the following disclaimer:

Baltimore County Public Schools (BCPS) makes every reasonable attempt to ensure that our school system’s Web sites are educationally sound and do not contain links to any content that can be deemed in violation of the BCPS technology acceptable use policy. Linked sites are not under the control of BCPS, but are provided as a convenience and do not imply an endorsement of the linked Web site or its contents. BCPS is not responsible for Web content accessibility of linked sites.

D. The Department of Information Technology will provide, training, guidance and support to office/school Webmasters. The design, content and
development of school or office Web sites to ensure compliance with Board policies and Superintendent’s rules.

E. School/office Webmasters shall post only official school and office Web sites on the BCPS network and services authorized by BCPS.

F. Office/school/teacher Web sites shall not include nor imply endorsement of advertisements, businesses or products.

G. Office/school/teacher Web sites shall be built using the BCPS Web Content Management System (CMS) templates and follow guidelines established by the Department of Communications and Community Outreach.

XII. Loss or Theft of Technology Equipment

A. Employees and authorized users who are assigned technology equipment are responsible for the care of the equipment in their custody.

B. When an employee or authorized user considers technology equipment to be lost or stolen, the employee shall:
   1. Report the loss or theft to his/her immediate supervisor;
   2. Notify the Baltimore County Police Department and have the police department generate a police report for the theft of BCPS TECHNOLOGY equipment. The police report must directly mention the theft of the BCPS TECHNOLOGY equipment and the circumstances surrounding the loss;
   3. Report the loss or theft within 24 hours to the Office of EMPLOYEE ABSENCE AND Risk Management by completing a BCPS Property Loss/Damage Report Form and forwarding the form to the Office of Employee Absence and Risk Management;
   4. Report the loss or theft within 24 hours to the Department of Information Technology through the online service desk system; and
   5. Cooperate in the loss investigation.

C. Costs incurred due to negligence, or misuse, malicious destruction or theft of BCPS technology may be the financial responsibility of the negligent or culpable person(s).

XIII. Compliance
A. All authorized users shall adhere to Board Policy 4104, this Rule[,] AND school system procedures [and the terms and conditions contained in the access forms signed by the user as provided in Paragraph III(C)].


C. ACCESS TO BCPS TECHNOLOGY MAY BE TERMINATED AT ANY TIME BY THE SUPERINTENDENT/SUPERINTENDENT’S DESIGNEE, WITHOUT NOTICE.

D. [B.]Violations of Board Policy 4104, this Rule or school system procedures WILL BE CONSIDERED MISCONDUCT IN OFFICE AND may result in loss of access to BCPS technology, disciplinary action, up to and including termination and/or criminal prosecution or restitution.

E. [C.]Illegal activities will be reported to appropriate law enforcement authorities and may subject the violator to civil and criminal penalties or consequences.

XIV. TRAINING

A. THE DIVISION OF CURRICULUM AND INSTRUCTION WILL BE RESPONSIBLE FOR ENSURING ALL EMPLOYEES ARE INFORMED ANNUALLY OF THE TECHNOLOGY AND SOCIAL MEDIA ACCEPTABLE USE POLICY AND THIS RULE, ARE AWARE OF THEIR RESPONSIBILITIES UNDER THIS POLICY AND RULE AND COMPLETE ANNUAL COMPLIANCE TRAINING ON THE ACCEPTABLE USE OF TECHNOLOGY AND PROFESSIONAL SOCIAL MEDIA.

B. ALL EMPLOYEES SHALL BE REQUIRED TO RECEIVE COMPLIANCE TRAINING ON THE ACCEPTABLE USE OF
TECHNOLOGY AND PROFESSIONAL SOCIAL MEDIA AS PART OF THE DIVISION OF HUMAN RESOURCES’ ONBOARDING PROCESS AND EVERY YEAR THEREAFTER.

C. VERIFICATION OF EACH EMPLOYEE’S PARTICIPATION IN COMPLIANCE TRAINING ON THE ACCEPTABLE USE OF TECHNOLOGY AND PROFESSIONAL SOCIAL MEDIA SHALL BE FILED IN THE EMPLOYEE’S EMPLOYMENT RECORD IN THE EMPLOYEE’S SCHOOL OR OFFICE.

Legal References: 18 U.S.C. §§ 2510-2522, Electronic Communications Privacy Act
20 U.S.C. § 794d, Section 508 of the Rehabilitation Act of 1973
20 U.S.C. § 1232g, Family Educational Rights and Privacy Act
47 U.S.C. § 254(h), Children’s Internet Protection Act
Annotated Code of Maryland, General Provisions Article §§ 4-101 to 4-601 (Public Information Act)
Annotated Code of Maryland, Labor and Employment Article § 3-712, Employers Prohibited from Requiring Disclosure of Employee User Names or Passwords to Personal Accounts or Services
COMAR 13A.05.04.01, Public School Library Programs

Related Policies: BOARD OF EDUCATION POLICY 0100, EQUITY
Board of Education Policy 1100, Communication with the Public
Board of Education Policy 1110, Publications, Radio, Television and Digital Media
BOARD OF EDUCATION POLICY 2380, RECORDS INFORMATION MANAGEMENT
Board of Education Policy 3125, School Activity Funds
Board of Education Policy 4002, Obligations of Employees of the Board of Education of Baltimore County
Board of Education Policy 4008, Board Data Governance
Board of Education Policy 4100, Employee Conduct and Responsibilities
BOARD OF EDUCATION POLICY 4102, SEXUAL HARASSMENT
BOARD OF EDUCATION POLICY 4103, CHILD ABUSE AND NEGLECT
Board of Education Policy 5230, Student Records
Board of Education Policy 6202, Technology Acceptable Use Policy (TAUP) for Students
RULE 4104

BOARD OF EDUCATION POLICY SUB SERIES 8360, ETHICS CODE [Board of Education Policy 8363, Conflict of Interest – Prohibited Conduct]

Related Rules: Superintendent’s Rule 2373, Public Information Act Requests
SUPERINTENDENT’S RULE 2380, RECORDS RETENTION
SUPERINTENDENT’S RULE 3125, SCHOOL ACTIVITY FUNDS

Rule

Superintendent of Schools

Approved: 06/09/97
Revised: 03/11/03
Revised: 04/22/08
Edited: 07/01/11
Revised: 03/11/14
Edited: 09/23/14 (Effective: 10/01/14)
Revised: 05/09/17
Revised: 08/20/19
REVISED: ______