RULE 4104

PERSONNEL: Conduct

Technology Acceptable Use Policy (TAUP) for Employees and Approved Non-Employees

I. Purpose

To implement Policy 4104 by establishing guidelines for the use of technology and social media by employees and approved non-employees in Baltimore County Public Schools (BCPS).

II. Definitions

A. *Authorized User* – Any employee or approved non-employee who has been authorized by the school principal or office head to have access to BCPS technology in order to carry out their duties for the school system.

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

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

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

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

F. *Non-Employee* – A volunteer, intern, independent contractor or an individual working for BCPS under a consultant agreement or purchase order and paid through the Department of Fiscal Services.

G. *Social Media* – 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.

H. *Technology* – 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.

III. Access Approval Process

A. Principals or office heads are responsible for determining when temporary employees and non-employees will have access to, and privileges on, BCPS technology. The principal or office head will determine which level(s) of access is required in order for the individual to perform his/her assigned duties.

B. Authorized users will be provided with a copy of Board of Education of Baltimore County (Board) Policy 4101, *Technology Acceptable Use Policy (TAUP) for Employees and Approved Non-Employees* and this rule and will be required to sign the technology forms for each authorized level of access prior to using or connecting to BCPS technology and the Internet.

C. Required Forms
1. Level 1: Internet
a. Prior to using or connecting to the Internet, authorized users will be required to sign the *Acceptable Use Agreement for Employees and Approved Non-Employees* (See, Rule 4104, Form A).
(1) The signed acceptable use agreement will be maintained as follows:
(a) Regular and temporary employees – in the employee's official personnel file in the Department of Human Resources.
(b) Independent contractors or any individual – 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 will be required to sign the *BCPS Electronic Mail Application Form* (See, Rule 4104, Form C).
(1) The Department of Information Technology shall retain all signed e-mail application forms.

b. Authorized users will be 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 will be required to sign the *BCPS Webmaster Agreement Form* (See, Rule 4104, Form B).

(1) Persons authorized under this paragraph shall be required to attend annual training.

(2) The Department of Information Technology shall retain all signed Webmaster forms.

D. For each level of authorized access, the Department of Information Technology will advise the authorized user when access has been granted and provide the user with applicable sign-on instructions.

IV. Guidelines

A. Any and all computer hardware, software, electronic files, peripheral devices and technology owned and leased by BCPS are to be considered under 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 BCPS-sanctioned student use of technologies.

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

VI. Social Media

A. Employees are required to use social media sites solely for BCPS' educational and school-related purposes, whether in connection with lessons and assignments or to facilitate communication within BCPS and the community.

B. Employees are prohibited from utilizing their personal social media accounts and/or Web sites for official school purposes.

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*. Teachers are required to comply with parental privacy options for the release of a student's directory information 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 to be 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 their particular school.

E. Professional social media communication must be in compliance 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. Crowdfunding

A. Employees wishing to raise funds for a particular school or classroom by use of donation-based crowdfunding 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. Employees shall comply with fundraising procedures established by the Department of Fiscal Services.

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:
   1. Bypass the school system's Web content filter;
   2. Access, upload, download, distribute, or communicate pornographic or sexually-explicit images, language or the files which generate such images or language;
   3. Create or communicate abusive, harassing, bullying, libelous, obscene, offensive, profane, threatening, discriminatory or illegal communications;
   4. Use technology for general personal use, personal gain or profit, lobbying, commercial or illegal purposes;
   5. 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.

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 that deal with school system business, may be subject to disclosure. Requests for public information will be handled in accordance with Superintendent's Rule 2373, *Public Information Act Requests*.

X. General Provisions

A. BCPS reserves the right to exercise editorial control over:
   1. All electronic publications and communications on all BCPS technology; 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. 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 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 of Education 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:

We have made every reasonable attempt to ensure that our school system's Web sites are educationally sound and do not contain links to any questionable material or anything that can be deemed in violation of the BCPS technology acceptable use policy. The 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.

D. The Department of Information Technology will provide, training, guidance and support to office/school Webmasters in 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 of theft to his/her immediate supervisor;
2. Notify the police department and generate a police report for the theft, or disappearance, of equipment. The police report must directly mention the loss of the equipment and the circumstances surrounding the loss;
3. Report the loss or theft within 24 hours to the Office of Risk Management by completing a *BCPS Property Loss/Damage Report Form* and forwarding the form to the Office of 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 that result in the malicious destruction or theft of BCPS technology will 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, school system procedures and the respective terms and conditions contained in the access forms signed by the user as provided in Paragraph III(C).

B. Violations of Board Policy 4104, this rule or school system procedures may result in loss of access to BCPS technology, disciplinary action, up to and including termination, and/or legal action.

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

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 §3-713, *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 1100, *Communication with the Public*
Board of Education Policy 1110, *Publications, Radio, Television, and Digital Media*
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, *Data Governance*
Board of Education Policy 4100, *Employee Conduct and Responsibilities*
Board of Education Policy 5230, *Student Records*

Board of Education Policy 6202, *Technology Acceptable Use Policy (TAUP) for Students*
Board of Education Policy 8363, *Conflict of Interest – Prohibited Conduct*

Related Rule: Superintendent's Rule 2373, *Public Information Act Requests*

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