STUDENT NAME:_____ **SCHOOL:** _____
TEACHER/HR: _____

ECPPS STUDENT TECHNOLOGY RESPONSIBLE USE

EXPECTATIONS FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

The use of school system technological resources, including access to the Internet, is a privilege, not a right. Individual users of the school system's technological resources are responsible for their behavior and communications when using those resources. Responsible use of school system technological resources is use that is ethical, respectful, academically honest, and supportive of student learning. Each user has the responsibility to respect others in the school community and on the Internet. Users are expected to abide by the generally accepted rules of network etiquette. General student and employee behavior standards, including those prescribed in applicable board policies, the Code of Student Conduct, and other regulations and school rules, apply to use of the Internet and other school technological resources. In addition, anyone who uses school system computers or electronic devices or who accesses the school network or the Internet using school system resources must comply with the additional rules for responsible use listed below. These rules are intended to clarify expectations for conduct but should not be construed as all-inclusive.

I acknowledge that I have read and understand the policies included in this document, including but not limited to: Policy Code: 3225/4312/7320 Technology Responsible Use, Policy Code: 3226/4205 Internet Safety, and Policy Code: 4318 Use of Wireless Communication Devices . I hereby agree to strictly comply with the terms and conditions of the above stated policies and rules - communicating over the network in a responsible manner while honoring all relevant laws and restrictions.

I further agree to be responsible for any school technology equipment or device that I am allowed to use during the school day. I will promptly report any issues with or damage to the device to my teacher. If I am assigned a device to use during the school day, I will be responsible for following established procedures for returning the device each day.

Before using school system technological resources, students and employees must sign a statement indicating that they understand and will strictly comply with these requirements and acknowledging awareness that the school system uses monitoring systems to monitor and detect inappropriate use of technological resources and tracking systems to track and recover lost or stolen equipment. Failure to adhere to these requirements will result in disciplinary action, including revocation of user privileges. Willful misuse may result in disciplinary action and/or criminal prosecution under applicable state and federal law.

PLEASE SIGN AND RETURN <u>TOP SHEET ONLY</u> TO YOUR SCHOOL MEDIA CENTER.

_____	_____	_____
Printed Student Name	**Student Signature**	**Date**
_____	_____	_____
Printed Parent Name	**Parent Signature**	**Date**
_____	_____	
School	**Teacher/Homeroom**	

Implemented: June 2 4, 2002
Revised: April 22, 2013
August 1, 2016

RETURN TOP SHEET ONLY

ECPPS STUDENT TECHNOLOGY RESPONSIBLE USE

Policy Code: 3225/4312/7320 Technology Responsible Use

RULES FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

1. School system technological resources are provided for school-related purposes only. Acceptable uses of such technological resources are limited to responsible, efficient, and legal activities that support learning and teaching. Use of school system technological resources for commercial gain or profit is prohibited. Student personal use of school system technological resources for amusement or entertainment is also prohibited. Because some incidental and occasional personal use by employees is inevitable, the board permits infrequent and brief personal use by employees so long as it occurs on personal time, does not interfere with school system business, and is not otherwise prohibited by board policy or procedure.
2. Under no circumstance may software purchased by the school system be copied for personal use.
3. Students and employees must comply with all applicable laws, including those relating to copyrights and trademarks, confidential information, and public records. Any use that violates state or federal law is strictly prohibited. Plagiarism of Internet resources will be treated in the same manner as any other incidents of plagiarism, as stated in the Code of Student Conduct.
4. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally viewing, accessing, downloading, storing, printing, or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages, or other material that is obscene, defamatory, profane, pornographic, harassing, abusive, or considered to be harmful to minors.
5. The use of anonymous proxies to circumvent content filtering is prohibited.
6. Users may not install or use any Internet-based file sharing program designed to facilitate sharing of copyrighted material.
7. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).
8. Users must respect the privacy of others. When using e-mail, chat rooms, blogs, or other forms of electronic communication, students must not reveal personal identifying information or information that is private or confidential, such as the home address or telephone number, credit or checking account information, or social security number of themselves or fellow students. For further information regarding what constitutes personal identifying information, see policy 4705/7825, Confidentiality of Personal Identifying Information. In addition, school employees must not disclose on school system websites or web pages or elsewhere on the Internet any personally identifiable, private, or confidential information concerning students (including names, addresses, or pictures) without the written permission of a parent or guardian or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA) or policy 4700, Student Records. Users also may not forward or post personal communications without the author's prior consent.
9. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks, or data of any user connected to school system technological resources. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance. Users must scan any downloaded files for viruses.
10. Users may not create or introduce games, network communications programs, or any foreign program or software onto any school system computer, electronic device, or network without the express permission of the technology director or designee.
11. Users are prohibited from engaging in unauthorized or unlawful activities, such as "hacking" or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems, or accounts.
12. Users are prohibited from using another individual's ID or password for any technological resource without permission from the individual. Students must also have permission from the

teacher or other school official.
13. Users may not read, alter, change, block, execute, or delete files or communications belonging to another user without the owner's express prior permission.
14. Employees shall not use passwords or user IDs for any data system (e.g., the state student information and instructional improvement system applications, time-keeping software, etc.) for an unauthorized or improper purpose.
15. If a user identifies a security problem on a technological resource, he or she must immediately notify a system administrator. Users must not demonstrate the problem to other users. Any user identified as a security risk will be denied access.
16. Teachers shall make reasonable efforts to supervise students' use of the Internet during instructional time.
17. Views may be expressed on the Internet or other technological resources as representing the view of the school system or part of the school system only with prior approval by the superintendent or designee.

PARENTAL CONSENT

The board recognizes that parents of minors are responsible for setting and conveying the standards their children should follow when using media and information sources. Accordingly, before a student may independently access the Internet, the student's parent must be made aware of the possibility that the student could obtain access to inappropriate material while engaged in independent use of the Internet. The parent and student must consent to the student's independent access to the Internet and to monitoring of the student's Internet activity and e-mail communication by school personnel.
In addition, in accordance with the board's goals and visions for technology, students may require accounts in third party systems for school related projects designed to assist students in mastering effective and proper online communications or to meet other educational goals. Parental permission will be obtained when necessary to create and manage such third party accounts.

PRIVACY

Students, employees, visitors, and other users have no expectation of privacy in anything they create, store, send, delete, receive, or display when using the school system's network, devices, Internet access, email system, or other technological resources owned or issued by the school system, whether the resources are used at school or elsewhere, and even if the use is for personal purposes. Users should not assume that files or communications created, transmitted, or displayed using school system technological resources or stored on servers or on the storage mediums of individual devices will be private. The school system may, without notice, (1) monitor, track, and/or log network access, communications, and use; (2) monitor and allocate fileserver space; and (3) access, review, copy, store, delete, or disclose the content of all user files, regardless of medium, the content of electronic mailboxes, and system outputs, such as printouts, for any lawful purpose. Such purposes may include, but are not limited to, maintaining system integrity, security, or functionality, ensuring compliance with board policy and applicable laws and regulations, protecting the school system from liability, and complying with public records requests. School system personnel shall monitor online activities of individuals who access the Internet via a school-owned device.
By using the school system's network, Internet access, email system, devices, or other technological resources, individuals consent to have that use monitored by authorized school system personnel as described in this policy.

ECPPS STUDENT TECHNOLOGY RESPONSIBLE USE

USE OF PERSONAL TECHNOLOGY ON SCHOOL SYSTEM PROPERTY
Each principal may establish rules for his or her school site as to whether and how personal technology devices (including, but not limited to smart phones, tablets, laptops, etc.) may be used on campus. Students' devices are governed also by policy 4318, Use of Wireless Communication Devices. The school system assumes no responsibility for personal technology devices brought to school.
Personal technology devices should not be connected to the school system's wired network

Though school personnel generally do not monitor students' Internet activity conducted on non-school system devices during non-school hours, when the student's online behavior has a direct and immediate effect on school safety or maintaining order and discipline in the schools, the student may be disciplined in accordance with board policy (see the student behavior policies in the 4300 series).

Policy Code: 4318 Use of Wireless Communication Devices
Students are permitted to possess such devices on school property so long as the devices are not activated, used, displayed, or visible during the instructional day or as otherwise directed by school rules or school personnel.

AUTHORIZED USE
Administrators may authorize individual students to use wireless communication devices for personal purposes when there is a reasonable need for such communication. Teachers and administrators may authorize individual students to use the devices for instructional purposes, provided that they supervise the students during such use.
Although use generally is permitted before and after school, use of cellular phones and other wireless communication devices may be prohibited on school buses when noise from such devices interferes with the safe operation of the buses. In addition, elementary and middle school students who participate in after-school programs are prohibited from using wireless communication devices during such programs.

CONSEQUENCES FOR UNAUTHORIZED USE
School employees may immediately confiscate any wireless communication devices that are on, used, displayed, or visible in violation of this policy. Absent compelling and unusual circumstances, confiscated wireless communication devices will be returned only to the student's parent.
The disciplinary consequences for violations of this policy shall be consistent with Section D of policy 4300, Student Behavior Policies. The superintendent or designee shall list in the Code of Student Conduct the specific range of consequences that may be imposed on a student for violations of this policy.
The following factors should be considered when determining appropriate consequences: whether the wireless communication device was used (1) to reproduce images of tests, obtain unauthorized access to school information, or assist students in any aspect of their instructional program in a manner that violates any school board policy, administrative regulation, or school rule; (2) to bully or harass other students; (3) to send illicit text messages; (4) to take and/or send illicit photographs; or (5) in any other manner that would make more severe disciplinary consequences appropriate.

SEARCH OF WIRELESS COMMUNICATION DEVICES
In accordance with policy 4342, Student Searches, a student's wireless communication device and its contents, including, but not limited to, text messages and digital photos, may be searched whenever a school official has reason to believe the search will provide evidence that the student has violated or is violating a law, board policy, the Code of Student Conduct, or a

school rule. The scope of such searches must be reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the suspected infraction.

LIABILITY

Students are personally and solely responsible for the security of their wireless communication devices. The school system is not responsible for the theft, loss, or damage of a cellular phone or other personal wireless communication device.