Crenshaw County Board of Education

Mr. J. Steven Sanders, Board President
Mr. Troy Hudson
Mrs. Bertha Jones
Mr. Steve Jackson
Dr. Charles S. Tompkins

Boyd K. English, Ed. D
Superintendent of Schools

Crenshaw County Board of Education

183 Votec Drive

Luverne, AL 36049
Phone (334) 335-6519
Fax (334) 335-6510
ccboe@crenshaw-schools.org
http://www.crenshawcounty.schoolinsites.com

CRENSHAW COUNTY PUBLIC SCHOOL SYSTEM
ELECTRONIC RESOURCES ACCEPTABLE USE POLICY

INTRODUCTION

The following policy relates to the acceptable use of the School System's electronic resources including devices, software, and networks by students. Prior to use of School System electronic resources, individuals shall read this policy and sign the required Acceptable Use Policy Contract.

A. General Use

1. Access to and use of Crenshaw County Public School System ("System") technology resources, including Internet and e-mail service, is a limited privilege, not a right. Students must adhere to System policies and procedures, federal, state and local laws, including, but not limited to, laws regarding libel, harassment, cyber bullying, theft, privacy, copyright, and threats. All of the System's policies apply to electronic use. Students who use System electronic resources and/or have remote access, have the responsibility to respect and follow the guidelines set forth herein and to honor the ethical norms associated with the highest standards of conduct. The System may restrict or suspend user privileges while any alleged violation(s) is being investigated and adjudicated. Failure to comply with School Board policies and state and federal guidelines may result in the loss of access and use of electronic resources, disciplinary action by the System, and civil and/or criminal prosecution.

2. No student has the expectation of privacy as to Internet, e-mail or computer usage. The System, either directly or with the assistance of a technology vendor, may monitor devices, systems, the Internet, e-mail and network traffic at any time. The System reserves the right to inspect any and all files stored on any network or local computer system, including removable media, such as diskettes, CDs, DVDs, tapes, and USB drives regardless of ownership. Students should be aware that their communications are stored within System electronic resources, including deleted communications, and these communications may constitute public records, business records, with which the System must comply. Further, the System holds and does reserve the right to inspect, copy, remove, lock out any data or file, or terminate guidelines, law or other School Board policy.

3. Accessing and/or transmission of any material deemed to be in violation of any federal, state or local law is prohibited.

4. The System will provide a standard device configuration with a charger in a protective cover. Unauthorized changes to the configuration are not allowed and removal of the device from the cover for any reason is prohibited.

5. Devices should be connected to a charging unit at the end of each day. All devices will be fully charged and ready at the start of each school day.

6. The device must be secured with the student's 4-digit secret password. Under no circumstance should the password be shared with another student. Each device must

automatically shut down when idle for 10 minutes. This setting may not be changed.

7. Examples of unauthorized general computer activities include, but are not limited to:
    a. Engaging in any illegal or inappropriate activities;
    b. Using school issued devices for storing of inappropriate content;
    c. Creating security breaches including, but not limited to: intentionally sharing passwords with unauthorized individuals; unauthorized access of confidential information or of data not intended for students; or logging into a server or account that the student is not expressly authorized to access;
    d. Revealing your personal information and that of another, such as the home address, telephone number, or Social Security number;
    e. Circumventing, reconfiguring or otherwise subverting system and network security measures, including, but not limited to, disabling antivirus software, performing port scanning or security scanning or the unauthorized execution of any form of network monitoring which will intercept data not intended for the student;
    f. Sending/receiving messages, requesting information or material, or accessing information or material that is fraudulent, harassing, obscene, offensive, discriminatory, lewd, sexually suggestive, sexually explicit, pornographic, intimidating, defamatory, derogatory, violent, or which contains profanity or vulgarity, regardless of intent.
    g. Messages containing jokes, slurs, epithets, pictures, caricatures, or other material demonstrating animosity, hatred, disdain, or contempt for a person or a group of people because of race, color, age, national origin, gender, religious or political beliefs, marital status, disability, sexual orientation or any other classification protected by law;
    h. Sending/receiving messages, viewing or requesting information reflecting or containing chain letters or any illegal activity, including, but not limited to, gambling;
    i. Any violation of items 7. a. - h. must be reported immediately to school personnel. Items not reported may subject a student to disciplinary action.

8. In the event of a security breach or suspected security breach, resulting from theft or loss of data, unauthorized access of data, System-wide malware or virus outbreak, or any method of “hacking”, school personnel should be notified immediately. Additionally, lost or stolen computers and devices must be reported to school personnel immediately.

9. The System is required to provide Internet content filtering in an attempt to keep inappropriate electronic media out of the classroom. No content filtering system can exclude all offensive material. Any site deemed inappropriate should be reported to school personnel immediately. Any unauthorized attempt to bypass or tamper with the filter is a violation of this policy and should be reported to school personnel immediately.

10. All websites created by students, or sanctioned school group representatives, created for any school related purpose (not limited to, but including the following: class assignment, class website, group or club promotion, sports, and band are required to be housed and stored on System-provided web servers or third party web hosting providers approved by

the System. The Superintendent has the right to terminate any System website at any time for any reason.

11. The System, independently or through contracted technology vendors, has the right to remotely monitor network traffic and computer workstations for the purpose of maintaining the security of the network, troubleshooting computer repair, and assisting students with technology related problems. Students shall not be notified before monitoring or remotely accessing the student's computer. The System recognizes that access to confidential information may be given to non-System employees in this process.

B. Internet Use

1. Software may not be downloaded from the Internet without specific authorization from the Information Systems Department.

2. Internet usage is subject to monitoring by the System and other external entities.

3. Students should not attempt to hide improper activity by deleting audit trails, history files and/or cookies, which store information related to Internet activity.

4. It is imperative that good judgment shall be utilized in viewing non-school related sites, and such utilization shall not impact the performance of the System's information technology resources, the student's work performance, nor result in any additional cost to the System.

5. Examples of <u>unauthorized</u> Internet activities include, but are not limited to:

    a. Engaging in any illegal activities;
    b. Installing, introducing, downloading, accessing or distributing unlicensed or unapproved software;
    c. Installing, introducing, downloading, accessing or distributing malware of any form (including viruses, worms, etc.) through willful intent or negligence (No file received from an unknown source shall be downloaded, whether attached to an e-mail message or downloaded from the Internet.);
    d. Downloading large files such as games, videos unless specifically needed in performing school work;
    e. Visiting any inappropriate website (sexually suggestive, violent, obscene, or vulgar material; inappropriate language or profanity; racial or otherwise discriminatory content);

C. E-mail Use

1. E-mail records are subject to the public record laws and other state and federal laws. Students may not harass, threaten or otherwise harm others by sending obscene, abusive, CAN-SPAM, or injurious messages. Sending or forwarding spam (i.e., electronic chain letters or junk mail) is not allowed.

<u>ANY BREACH OF THIS POLICY IS PUNISHABLE IN ACCORDANCE WITH THE RULES SET FORTH IN THE CRENSHAW COUNTY PUBLIC SCHOOL SYSTEM'S CODE OF CONDUCT & STUDENT HANDBOOK.</u>

CRENSHAW COUNTY PUBLIC SCHOOL SYSTEM
ELECTRONIC ACCEPTABLE USE POLICY CONTRACT

Student Name _____ Address _____
Phone: _____ Alternate Phone _____
Parent/Guardian Name _____Address _____
Home Phone _____ Other Phone _____

I understand that a School System take-home device with cover will be issued for (Name of Student) _____ at _____School. The device is capable of Internet access that is filtered while at school. I understand that it is my responsibility as parent/guardian to monitor and control my child's use of the device while away from school. I further understand that inappropriate use is a violation of the Crenshaw County Board of Education Student Handbook & Code of Conduct.

I have examined and tested the device identified below, and find it to be in good working condition. I understand that the device, like textbooks, is instructional material, and that I am legally responsible for the replacement cost if it is lost, stolen, or damaged beyond repair. I agree to return the device in good working order to _____ School at the end of the school year as directed.

I agree to pay the School System an insurance fee of twenty-five dollars ($25) prior to receiving the device to cover accidental damage. A $25 deductible will be charged for a first repair and a $50 deductible for a second repair. Exclusions from insurance coverage are: (1) neglect, abuse or intentional damage or loss; (2) any intentional, dishonest, fraudulent or criminal act which results in damage or loss; (3) inappropriate use as defined by the Student Code of Conduct or School Board policy; (4) damaged when taken out of the cover. No more than two devices will be provided to a student during any one school year. Additional loss may result in forfeiture of use of the device by the student or other penalties at the discretion of the school.

ANY BREACH OF THIS CONTRACT IS PUNISHABLE IN ACCORDANCE WITH THE RULES SET FORTH IN THE CRENSHAW COUNTY PUBLIC SCHOOL SYSTEM'S CODE OF CONDUCT & STUDENT HANDBOOK.

Student _____ Date _____
Parent/Guardian _____ Date _____

Serial Number	Asset Tag Number	Date Out	Date Returned	Working Condition

Adopted July 18, 2013