CUMBERLAND REGIONAL SCHOOL DISTRICT

ACCEPTABLE USE POLICY FOR DISTRICT TECHNOLOGY

FOR STUDENTS

2015-16 SCHOOL YEAR

PLEASE NOTE THAT AS OF THIS YEAR, WITH THIS FORM, ONLY ONE TECHNOLOGY AUTHORIZATION IS REQUIRED FOR A STUDENT'S ENROLLMENT AT THE CUMBERLAND REGIONAL HIGH SCHOOL DISTRICT, UNLESS THE PARENT/GUARDIAN CHOOSES TO CANCEL IT.

LAST UPDATED: FEBRUARY 2015

TABLE OF CONTENTS

PURPOSE

Cumberland Regional High School District (CRHSD) is pleased to offer students access to district computers, the Internet and an array of technology resources to promote educational excellence. Each student is responsible for his/her use of technology whether district-provided or privately-owned. While using district or privately-owned technology resources on or near school property, in school vehicles, and at school-sponsored events, as well as using district technology resources that are Internet-based (email, online storage, etc.), each student must act in a manner consistent with school, district and legal guidelines.

We would like to inform parents of the benefits of Internet access to students, and at the same time, advise parents of the potential for misuse which may result from access to the district-wide network and Internet.

Please note that the use of privately-owned technology in a classroom will be at the discretion of the individual classroom teacher; likewise, privately-owned technology use in the Instructional Media Center will be at the discretion of the Media Specialist. Use in other areas of the building will be at the discretion of CRHSD Administration.

The use of the CRHSD network is a privilege, not a right, and inappropriate use, including violations of these rules, may result in cancellation of the privilege. All district students, personnel, outside providers, and vendors are required to sign and follow the Acceptable Use Policy of network technology as outlined below.

Accessing the CRHSD network without authorization and/or attempting to access, alter or damage any part of the network, computers, data, etc., is a violation of state and federal law and may be reported or referred to law enforcement.

LIMITATION OF LIABILITY

The Internet constitutes an unregulated collection of resources that changes constantly, so it is not possible to totally predict or control the resources that users may locate. The board cannot guarantee the accuracy of the information or the appropriateness of materials that a user may encounter. Furthermore, the board shall not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. Nor shall the board be responsible for financial obligations arising through the unauthorized use of the system.

ACCEPTABLE USE OF NETWORK TECHNOLOGY

- The computer system is the property of the district, and all computer software and hardware belong to the district.
- The District's local and wide area networks are intended only for educational use and for the business and administrative functions directly in support of the school district's operation.
- Personal use of network resources, including the Internet and e-mail, is prohibited.
- Network services and access to these services shall only be used by authorized persons. Where password-protected accounts are used, network users are personally responsible for all activity that occurs within their account.

- All users are expected to maintain privacy and confidentiality of district ~~network~~ accounts and passwords. Users are prohibited from sharing ~~network~~ accounts and passwords, which includes allowing others to use their password-protected account.
- Users are advised that computer systems are district property and may be inspected or monitored at any time consistent with district policies and federal laws.
- As required by the Children's Internet Protection Act ("CIPA"), the district will monitor students' online activities. Such monitoring may lead to discovery that the user has violated or may be violating the District's Technology Acceptable Use Policy, the student disciplinary code or the law. The District also reserves the right to monitor other users (e.g., non-students) online activities.
- At no time can privately-owned technology be physically attached to district-owned equipment or district network interfaces.
- All students are prohibited from connecting to district wireless networks with any privately owned technology unless a waiver for the privately owned technology has been signed and approved by the Technology Systems Manager. In addition, students and parents must sign this Acceptable Use Agreement.
- Users of the district network and computers and other hardware are expected to use the equipment with diligence and care. Any vandalism or malicious damaging of the equipment may result in the loss of network access, restricted use of district equipment, and restitution for the damaged equipment.
- Other disciplinary action may be imposed as stated in the CRHS Student Handbook.
- Users shall immediately notify the Technology Systems Manager if they detect a possible security problem. Users shall not access the system solely for the purpose of searching for security problems. Users shall not install or download software or other applications without express permission from the Technology Systems Manager. Users shall also follow all district virus/malware protection procedures when installing or downloading approved software.

PERSONAL SAFETY VIOLATIONS

Users will

- Not post personal contact information about themselves or other people using district resources:
    - Personal contact information includes name, home address, telephone numbers, school address, work address, etc.;
    - Postings include e-mails, messages, and text or graphics placed on websites.
- Promptly disclose to the teacher or other school employee any message a student receives that is inappropriate or makes the student feel uncomfortable;
- Not use district resources to correspond with individuals online, unless for school related purposes or if directed to do so by a district staff member;
- Not use district resources or personal resources while in school to send or receive sexually explicit messages.

INTERNET SAFETY AND CYBER-BULLYING

Cyber-Bullying is defined as the willful and repeated act of harming others electronically, through e-mail, instant messaging, web sites, chat rooms, social networking sites, cell phones and other electronic means.

Users will not

- Use district technology to deface, harass or demean others;
- Provide personal information on the Internet;

- Send or retrieve inappropriate material using computers, mobile devices such as iTouch/iPods, cell phones, e-mail, blogs, newsgroups or any other electronic means;
- Use district resources to defame the character or credibility of a person;
- Participate in inappropriate uses of district resources and network files in school that disrupt the normal educational process of the school; and
- Send or post messages using another person's profile or taking on the identity of another person.

PROHIBITED ACTIVITIES

Users will not

- Transmit material that
    - is threatening to the safety of another person; and
    - could be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, disability, religion or political beliefs.
- Vandalize district technology including hardware and software. Vandalism is defined as any malicious or intentional attempt to harm or destroy data of another user, the destruction of computer equipment or other property, or the theft or defacing of computer equipment. This also includes the intentional uploading or creation of computer viruses, spyware, malware or other malicious, destructive or disruptive programs. Vandalism will result in cancellation of privileges and possible disciplinary or legal action;
- Transmit or view obscene or pornographic material, hate messages, and/or any unlawful material;
- Use network resources to commit unlawful offenses;
- Override or attempt to override any security measures established on the network or encourage others to do so;
- Access or attempt to access any prohibited sites;
- Use the network system for soliciting or distributing information with the intent to harass, intimidate, or bully which can be described as Cyber-Bullying;
- Post chain letters or engage in "spamming"' that is, sending an annoying or unnecessary message to multiple recipients;
- Use abusive, profane, obscene, harassing, racist or other inappropriate language;
- Post information that, if acted upon, could cause damage or disruption in the normal operation of the school;
- Engage in personal attacks, including prejudicial or discriminatory attacks;
- Harass another person; harassment is persistently acting in a manner that distresses or annoys another person;
- Knowingly or recklessly post false or defamatory information about a person or organization;
- Take, post, or publish pictures or videos in classrooms, locker rooms, hallways, or other areas of the school, as well as at school-sponsored activities, or on school-provided transportation to/from those activities, of staff members or other students without the knowledge and consent of district staff and written approval from the parents of all students involved;
- Access blogs, wikis, social network sites, news groups and other means of collaboration unless it is a staff sponsored resource that is used for school purposes;
- Use district resources to access personal e-mail; and
- Use district resources to search the Internet for non-educational purposes.

PLAGIARISM AND COPYRIGHT INFRINGEMENT

Users will not

- Plagiarize works that they find on the Internet.
  District policies on plagiarism will govern use of material accessed through the district system. Teachers will instruct students on appropriate research and citation practices;
- Install illegal copies of copyrighted software. The district will adhere strictly to all software copyright and licensing laws; and
- Download or burn copyrighted material using district resources.

SECURITY

- Passwords must not be exchanged and other's passwords must not be used. The individual is responsible for the security of his/her own password.
- Attempts to log into any network system as any other user will result in cancellation of user privileges.
- Attempts to log in as a system administrator may result in the cancellation of user privileges.
- Use of another individual's password-protected account is prohibited; allowing another individual to use your password-protected account also is prohibited.
- Trespassing, deleting, or changing another other student's folders, work, or files is prohibited and may result in cancellation of network access and privileges.
- Users' shall not use the network for any illegal activity including, but not limited to, unauthorized access including hacking.

ELECTRONIC MESSAGES AND POSTINGS

E-mail is defined as point-to-point messages, posting to newsgroups and any electronic messaging involving computers or computer networks.

- E-mail is provided for the purpose of exchanging information consistent with the mission of the district.
- School-issued accounts for e-mail and collaborative projects must only be used for school-related purposes.
- Correspondence between students and staff members must use only the school-issued accounts, not personal ones.
- While engaged in activities on the district network users are prohibited from transmitting e-mail to others that includes material that is vulgar, rude, obscene, pornographic, inflammatory, threatening, harassing, disrespectful, or which uses sexually explicit language.
- Users are prohibited from posting chain letters or sending spam messages to users on the network or while using network resources.
- E-mail is subject to the New Jersey records law to the same extent as it would be on paper communication.
- Users will practice appropriate Internet etiquette when using electronic communication resources such as school e-mail, blogs, wikispaces, and other social media.
- Information may not be posted if it: violates the privacy of others, jeopardizes the health or safety of students or staff, is obscene or libelous, causes disruption of school activities, plagiarizes the work of others, is a commercial advertisement, or is not approved by School Administration.

User Responsibilities:

- Your district e-mail account is for your use only and no one else may use your account.
- Users may be held liable for deleting computer data that is subject to legal prosecution.

CONSEQUENCES OF VIOLATION

In the event there is an allegation that a student has violated the District Acceptable Use Policy, he/she may be subject to disciplinary action as outlined in their Student Handbook. Users and/or their parents or guardians may be held financially responsible for losses, costs, or damages to any school computer or system.

Penalties will be administered based on the severity and frequency of the offense. The district will assign penalties after consultation with the staff member involved and the Principal.

It is every student's responsibility to cooperate in any investigation of a complaint or alleged violation of the policy by providing any information he/she possesses concerning the matters being investigated. Further, it is against district policy to attempt to alter, delete or destroy documents, files, etc. that are the subject of investigation. Students should realize that the network administrator can still recover files which have been deleted.

Consequences to violations include but are not limited to

- Suspension of Internet access;
- Revocation of Internet access;
- Suspension of network privileges;
- Revocation of network privileges;
- Suspension of computer access;
- Revocation of computer access;
- School suspension;
- School expulsion;
- Paying fees and charges accrued as a result of damage or loss to the property before receiving copies of your school records;
- Restriction from participating in school activities; and
- Legal action and prosecution by the authorities.

Cumberland Regional School District has the right to restrict or terminate anyone's network and Internet access at any time for any reason. Further, Cumberland Regional School District has the right to monitor network activity in any form following board policies and federal laws that are deemed necessary to maintain the integrity of the network.

CUMBERLAND REGIONAL SCHOOL DISTRICT

Student Technology Acceptable Use Agreement

This form is to be completed by students and parents after reviewing the district Acceptable Use Policy. The completion of this form indicates that you have read the policy and understand the same. It also indicates that you agree to abide by the terms and conditions of the policy. This form must be signed both by you and a parent/guardian before you will be permitted to have access to the districts' network.

I understand and agree to accept and abide by the Student Technology Acceptable Use Policy. I also understand that if I fail to follow the policy, my access to the computer network, e-mail services and the Internet, may be suspended. I may be subject to other discipline, and there may even be criminal consequences to my behavior depending upon the severity of my actions.

All information must be completed and legible for this form to be accepted!

Student Signature: _____Date:_____

Student Name (**must be printed**):_____

Grade: _____

As a parent/guardian of the student above, I hereby give my permission for my child to access the district computer system which includes access to the Internet and school-issued e-mail. I have read the District Technology Acceptable Use Policy and I understand that my child is expected to abide by all policies described. I understand that the district is employing filtering software, but it is not always 100% effective. I understand that if arrangements are made to permit my child to access the district computer system from outside of school I am responsible to provide appropriate supervision.

I understand that all staff members are encouraged to have updated web pages for information and curricular reasons, which may include student photos/images/videos/names or student work; furthermore, that the district may post acknowledgements of student accomplishments or awards, or may feature students in district-created presentations, which may include student work or photos/images/videos/names. My signature below serves as permission to use these.

I also understand that all faculty members are encouraged to explore rich learning opportunities with their students by exposing them to classrooms across the world, and subject-matter experts who are local and abroad, through the use of video conferencing technologies such as SKYPE; furthermore, that there may be times when these sessions are recorded to be played back in the school district only, and that the school district will take all reasonable precautions to safeguard the videos from any third party and outside viewers. My signature below serves as permission for participation in distance learning activities.

I understand that this acknowledgement will apply for the rest of my child's schooling in the Cumberland Regional High School District unless I choose to cancel.

All information must be completed and legible for this form to be accepted!

Parent/Guardian Signature _____ Date _____

Parent/Guardian Name (**must be printed**) _____