Acceptable Use and Internet Safety Policy and Procedures for Information Systems at Castle Rock School District (CRSD)

Introduction

Policy 3202 and Procedure 3202P of Castle Rock School District #401 exist to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children’s Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

The intent of this policy and procedure is to promote responsible and ethical use of the network resources provided by Castle Rock School District. All use of the system must be in support of education and research and consistent with the mission of the district. The district reserves the right to prioritize uses and access to the system.

- Any use of the system must be in conformity with state and federal law, network provider policies and licenses, and district policy.
- The Superintendent or designee must approve use of the system for charitable purposes in advance.
- Use of the system for commercial solicitation is prohibited.
- The system constitutes public facilities and may not be used to support or oppose political candidates or ballot measures.
- Although these policies and procedures are written specifically with minors in mind, adult employees of legal age are expected to adhere to them unless a specific exception has been granted for research or investigative reasons by the Superintendent or designee.

Account Security

You are responsible for all activity that occurs with your account.

You are not permitted to use another individual’s account, and should never allow anyone else to access your account. If, at any time, you feel that your password may have been compromised, see the System Administrator immediately to have your password changed.

- Log out correctly when you leave your computer.
- Logged on computers should never be left unattended. Lock your computer with your password if you leave but intend to return shortly.

Good network security practices will require passwords to be changed for all accounts at regular intervals. Users should avoid easily guessed passwords. Password length must be 8 characters minimum on our system.

Security on any computer system is a high priority, especially when the system involves many users. If you identify a security problem on the network, notify your teacher, the System Administrator, or the principal. Do not purposely seek to identify security problems without consent from the System Administrator.
**Student Computer Accounts**

Students are expected to use network resources responsibly. Computer accounts and network storage are intended for classroom assignments and files created for educational purposes only.

- Storage of unauthorized games, computer programs, media downloads, or copyrighted materials are not permitted (Category B to C infraction).
- Use school appropriate file and folder names (Category B infraction and file removal).
- Never attempt to conceal or encrypt files on the network (Category C infraction).

The System Administrator has complete access to the content of all student folders. Students are granted access to their assigned file storage space only. Teachers are given read access to students’ folder space.

The System Administrator reserves the right to remove any material stored in computer files which, in his/her sole discretion, may be unlawful, obscene, in violation of copyright, or otherwise unrelated to the teaching and laboratory mission of the school. *For example: games, unauthorized programs, and media downloads.*

**Printing**

- Excessive printing without permission of a teacher or staff member is a violation. Permission is required for color printing.
- Wasteful printing may result in disciplinary actions and a fee to replace resources.
- Purposely using printers to send messages or harass will result in disciplinary actions.

**System Care**

Students are responsible for proper care and maintenance of computer equipment and peripherals.

- No food or drinks are allowed at any of the computer workstations.
- Students must avoid any activity around their workstation that may result in damage to the computer, printer, software, or information.
- No computer hardware, peripherals, or cables may be moved or removed from their current location without specific authorization by the System Administrator (Category B infraction).
- No student will attempt to service any hardware without authorization from the System Administrator (Category B infraction).
- Do not change system or display settings on computers without permission from the System Administrator.

**STUDENTS SHOULD REPORT ANY PROBLEMS WITH THE EQUIPMENT IMMEDIATELY.**

**Acceptable Use**

- Creation of files, projects, videos, web pages, and podcasts using network resources in support of educational research;
- Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and web pages that support educational research;
- With parental permission, the online publication of original educational material, curriculum-related materials and student work. Sources outside the classroom or school must be cited appropriately;
- Staff use of the network for incidental personal use in accordance with all district policies and guidelines;
Connection of personal laptops to the district network after checking with the System Administrator to confirm the laptop is equipped with up-to-date virus software, compatible network card and is configured properly. Connection of any personal electronic device is subject to all guidelines in this document.

Unacceptable Use of Computer System

- Use of the system to disrupt others or the normal operation of the system will not be tolerated; this includes illegal tampering, destruction of system hardware, altering system software, and unauthorized entry into computers. This kind of activity is a crime under state and federal laws.
- Students must not engage in any activity intended to circumvent computer security controls. Students must not attempt to crack passwords, discover unprotected files, or decode encrypted files; this also includes creating, modifying, and executing programs that are designed to hack computer systems (Category C infraction). *(CIPA)
- Attempts to login to the network as a System Administrator or gain unauthorized access will result in the cancellation of computer privileges.
- Using viruses, worms, Trojan horses, or any other invasive software is expressly forbidden (Category C infraction). **Punishable by federal law.**
- Students may not use the school's voice/data connections to harass anyone.
- Impersonating other users by using their accounts or login names will result in the restriction of the offender accounts. The impersonator will face review for discipline.
- While in classroom instruction or in a lab setting, computer and technology privileges are limited by the instructor or lab monitor. Each student is expected to use the technology in compliance with the instructor. No use of e-mail or Internet activity is allowed unless the instructor has authorized such use in the classroom. Each academic lab may impose additional rules not explicitly covered in this Acceptable Use Policy and Procedure. Failure to comply will be considered an infraction of the Computer Use Policy (Category B infraction).

Internet Acceptable Use

Students should have a specific reason to use the internet. The internet is provided for educational, not recreational purposes.

- Never attempt to download or install software programs on school computers. This includes browser plug-ins, media players, messaging software, ad-ware, games, or file-sharing utilities.
- Use of the system to access, store or distribute obscene or pornographic material is prohibited. *(CIPA)
- Sites that are gang-related or contain illegal or degrading information are prohibited.

If a student or staff member misuses the Internet as described in this Policy, the final decision on action taken will be at the discretion of School Administration.

Internet Monitoring and Filtering

Our schools utilize software to monitor and filter inappropriate web sites. No system can filter all inappropriate sites 100% of the time. This system is intended to help shield students from accidentally accessing inappropriate sites. STUDENTS SHOULD REPORT INAPPROPRIATE SITES ACCESSED OR NOT FILTERED IMMEDIATELY. *(CIPA)
The school filtering policies are set to block obscene materials, child pornography, and sites harmful to minors at a minimum. Under no condition will these filtering policies be relaxed for a minor. These kinds of filter policies apply to adults also but may be relaxed for investigative purposes authorized by the Superintendent, Principal, or System Administrator only. *(CIPA)*

**Site Review Requests** – The filtering systems block page provides a means to request a review of a site for the purpose of unblocking it. The System Administrator has sole discretion to allow or disallow sites on our school network. Decision will be made based on site appropriateness and educational merit. While every effort will be made to act on blocking and unblocking requests as quickly as possible, in some cases the review may take 3-5 days. Those submitting a request will be notified when a decision is made. The user must provide the exact URL (copy and paste into the e-mail) in order for the site to be reviewed.

High priority requests:

- Teacher originated requests with return e-mail.
- Respectfully written student requests.
- Obvious falsely blocked sites.
- Sites with exclusive information. Often the same information can be found on other sites.

Request Refusals:

- Requests with no return e-mail. Ask a teacher to submit a request if you have no e-mail account.
- Any request written with disrespect in any way. Disrespectful communications may be subject to referral.
- Requests ignoring proper writing conventions.
- Requests for known banned sites. *For example: “Myspace”*
- Any site that may distract from subject being taught in the classroom.
- Sites without educational merit. *For example: “South Park”, “Bored.com”, etc.*

Attempts to bypass the school’s filtering system are considered a form of hacking and will result in disciplinary actions. *For example: anonymous proxies, key loggers, programs on USB storage devices, etc.*

It is the student’s responsibility to not access sites in categories deemed inappropriate to the school setting. Just because a site is not blocked by the filtering system does not mean access is allowed.

**Electronic Communications** – includes e-mail, chat, instant messaging, forums, blogs, text messages, social networks, and other direct forms of electronic communications.

- Never use electronic communications during class time without permission. Category A infraction for the first offense and Category B infraction for all subsequent offenses.
- Students must not send any electronic communications by forging another's identity or attempting to conceal the origin of the message in any way.
- Students are prohibited from transmitting or forwarding chain letters, mass mailings, or SPAMMING (Category B infraction).
- Students may not access or attempt to access another person's e-mail (Category B infraction).
- Do not access electronic communications of any kind from someone you do not know.
- Never open e-mail attachments or download files that could contain viruses.
• Students are not to access chat rooms at school.
• Do not use command-line utilities to send messages to other users on the network.
• For reasons of system and personal security, each system account holder must authorize district review of e-mail messages.
• Participating in electronic communication services is only permissible for students under the appropriate supervision of a sponsoring teacher. The sponsoring teacher must gain permission for such activities from the Superintendent or designee. Sponsoring teachers must be trained in Internet safety procedures and educate minors about appropriate online behavior. Sponsoring teachers must actively monitor students while they are online in their classrooms and while using computer labs. *(CIPA)*

**Unacceptable Cell Phone and Computer Use by Staff**

Although it is desirable that staff members have a sincere interest in students as individuals, partiality and appearance of impropriety must be avoided. Excessive informal and/or social involvement with individual students is prohibited. This includes any calling, texting or e-mailing students in a social context. Such conduct is not compatible with professional ethics and, as such, will not be tolerated.

**E-mail Use**

E-mail creates a permanent record that may be archived and retrieved at a later date, even though the user has deleted it. E-mail is subject to the district document retention policy. Be cautious about what you send and to whom. E-mail is a public record which may be examined by any individual at any time.

• E-mail attachments may introduce viruses. Be cautious if you are unsure of the origin of an e-mail; if the e-mail includes an attachment, do NOT open it - delete it immediately.
• Staff members may not use their district-provided e-mail account for monetary gain, political/religious advocacy, union activities not approved by negotiated agreement, or private business enterprises.

**Etiquette**

You are expected to abide by the generally accepted rules of network etiquette.

• No use of obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
• Deliberate accessing, downloading and disseminating any material deemed offensive, obscene, racist, antisocial, homophobic or violent are expressly prohibited.
• Knowingly or recklessly posting false or defamatory information about a person or organization is expressly forbidden.
• Do not engage in harassment of another person. Harassment is persistently acting in a manner that distresses or annoys another person. Immediately cease any activity causing a person to feel harassed, upon notification from that person or school administration.

**YOU ARE A REPRESENTATIVE OF YOUR SCHOOL AND YOUR DISTRICT ON A PUBLIC SYSTEM.**

**Internet Safety**

• Students should never post **personal information about self or others** on the Internet (address, telephone, school, school address, work address, parent’s name, etc.).
• Students should never make appointments to meet people in person they have contacted online without district and parent permission.
• Students should promptly disclose to a teacher or to other school staff any message received that is inappropriate or makes them feel uncomfortable.
• Immediately report any personal attacks made by others to responsible school personnel. *(CIPA)

Publishing Student Information on the Web
• No home phone numbers or addresses of students may be published. *(CIPA)
• Students shall not include personal information that would permit others to determine the location of the student at any given time. This includes places of employment, specific times and dates of extracurricular activities, class schedules, and other information that poses a safety concern for the student. *(CIPA)
• Content on the web page(s) must comply with the internet user agreement
• Links to student web pages not located on the district web servers may not be made from the schools’ web pages.

Staff Use of Social Networking Sites
While you may use Facebook, Myspace, Twitter, or other social networking sites in your personal life, it is not appropriate to "accept" students as "friends" who may wander onto your page. If you have already accepted students onto your social networking page, please set a boundary for them to follow such as:

• All staff have been asked by the district to use district communication mechanisms to communicate with students. If you wish to contact me, my school e-mail address is: ____________ and my school voice mail is ____________. I look forward to working with you at school.

Copyrighted Materials
Users of the system must respect all copyright laws. Legal authorization must be obtained for the transfer, use, or duplication of copyrighted materials. Some examples of material that may be copyrighted are intellectual property, clip art, images, photo, video, sound, as well as software packages.

The duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and is cited appropriately.

• Students must not plagiarize works that are found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours.
• Students will not access, read, delete, or tamper with any file that is not theirs.
• Copying of any software, network or otherwise, is strictly prohibited. It is against the law and is punishable.
• Outside software is not permitted in any computer area; no software is to be downloaded, stored, or installed on any computer or in any computer account.
• Material posted on the Internet through the district’s system is not protected for individual copyright. Staff work is usually a work for hire with the copyright belonging to
the district, but all users must waive their copyright interest in their materials posted online through the district's system.

- All student work is copyrighted. Approval to publish any student work requires permission from the parent or guardian.

A copy of every school-owned software license must be kept in a secure file in the school, and another copy sent to the district Technology Director (System Administrator). The district reserves the right at any time, without notification, to uninstall, remove or delete any software, from any computer or network server, which does not comply with district software policy.

**Student Data is Confidential**

District staff shall maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).

**School Web Sites**

The school's computer system may be used to create, revise, and house home pages for the school, departments, school organizations/clubs, and personal home pages for the students, faculty, staff, administration, and board members. No other home page can be housed on the school's system without specific permission from the System Administrator (Category B infraction).

- Students or staff members who post, create, or build any web site linked to CRSD without the school’s knowledge or express permission will be subject to investigation by the System Administrator and possible disciplinary action. All such sites will be reviewed for purpose, nature and content.

**Disciplinary Action**

Use of school computers and the Internet are privileges, and unacceptable use may result in the cancellation of those privileges. Violation of any of the conditions of use explained in the district's user agreement, electronic resource policies, or these procedures could be cause for disciplinary action, including but not limited to suspension or expulsion from school and suspension or revocation of network and computer access privileges for students; and suspension and/or termination of employment for staff.

Depending on the severity of the violation (to be determined by the System Administrator and/or administration), computer privileges may be revoked for an extended period of time. A student who has his/her computer privileges revoked is not allowed to use any computer at her/his school site. Legal action and/or dismissal from school may result from violations of state or federal laws.

Routine maintenance and monitoring of the school computer system may lead to discovery that a policy has been violated. An individual search will be conducted if there is reasonable suspicion of a policy violation. The investigation will be reasonable and related to the suspected violation.

In the course of an investigation, private user-related information may be revealed to other employees or concerned parties. **Students may temporarily be denied access pending the review if there is a reasonable suspicion that the student may use his/her access to cause harm or do damage in the interim.**
Any misuse will result in loss of computer privileges, disciplinary action, or possible legal referral. Misuse is defined as any malicious attempt to physically deface, disable, or destroy computers, peripherals, or other network hardware; to harm or destroy data of another user or any other agencies or networks that are connected to the system; to gain access or attempt to gain access to unauthorized systems; or to access inappropriate materials from school computers. Misuse is not restricted to this definition. The school administration may require restitution from offending students for all damage, labor resulting from damage, or loss due to computer misuse or damage.

Penalties for computer infractions:

Category A infringements (non-malicious): Written warning or student may be given verbal warning.

Category B infringements: One or more day’s suspension of one or more network privileges.

Examples (not limited to):

- Use of chat rooms, newsgroups, Instant Messenger
- Continual use of non-school related sites after being warned
- Unauthorized use of e-mail after being warned
- Use of other student and staff logon information to access a computer
- Continued failure to log off when finishing use of a computer

Consequences

Loss of Internet privileges (still may use computer for other uses). The infringement and consequence will be reported to all staff. All staff will then provide consistency and follow through. Parents/legal guardians will be notified.

Category C infringements: Indefinite suspension of one or more network privileges and probation.

Examples (not limited to):

- Accidentally accessing offensive material and not exiting site immediately
- Using the Web for transactions that involve money
- Deliberately corrupting or destroying others data, violating privacy of others
- Repeated offense of any above infringements

Consequences

Loss of computer and Internet privileges for the semester or a period of time deemed appropriate by staff members involved. The infringement and consequence will be reported to all staff. All staff will then provide consistency and follow through. Parents/legal guardians will be notified and a discipline referral will be made. Referrals for Category C violations may result in short term suspension, long term suspension, and/or expulsion.

ANY TIME STUDENT’S MISUSE OR DAMAGE COMPUTERS, LAW ENFORCEMENT AGENCIES MAY BE NOTIFIED.

Disclaimer of Liability

Although the System Administrator will try to meet users’ needs and requests, there is no guarantee it will be done, nor that network services will be error free or uninterrupted. The System Administrator reserves the right to add, delete, edit and reconfigure files, accounts,
software and services as necessary to maintain and upgrade the network and its computers. The System Administrator will not be liable for any direct or indirect, incidental or consequential damages (including lost data), sustained in connection with the use, operation, or inability to use the network.

I will abide by such rules and regulations of network use as may be added from time to time by the System Administrator. These rules will be posted on public display in the computer laboratories and online.

*(CIPA) - Children’s Internet Protection Act – minimum policies requirement.

Adoption

This Acceptable Use and Internet Safety Policy and Procedure were adopted by the Board of Castle Rock School District #401 at a public meeting, following normal public notice, on December 22, 2009.

Chair, Board of Directors: Gayle Baker
Superintendent: Susan Barker