

Computer Technology Use Agreement
A Summary of the Acceptable Use and Internet Safety Policy, Administrative Guidelines and
Rules for Computer & Network Use

The Cresskill School District is pleased to make available to students access to computer technology, connectivity to the Internet and other district or associated networks, use of software programs and peripherals (henceforth also referred to collectively as “the system”, “network” or “technology resources”). The Internet or World Wide Web (WWW) is the worldwide network that provides various means of accessing significant educational materials and opportunities via a connected computing device.

In order for the School District to be able to continue to make these technology resources and connectivity available, all students must take responsibility for appropriate and lawful use of this system. Students must understand that one student’s misuse of the network and/or the Internet connection may jeopardize the ability of all students to enjoy such access. While the school’s teachers and other staff will make reasonable efforts to supervise student use of computers, network use and Internet access, they must have student cooperation in exercising and promoting responsible use of these resources.

In order to maintain and encourage appropriate and effective use of computer technology and connectivity, the Cresskill Public Schools have defined a set of RULES FOR COMPUTER AND NETWORK USE and an ACCEPTABLE USE AND INTERNET SAFETY POLICY (henceforth referred to as COMPUTER RULES and AUP respectively). The AUP is part of a series of Board of Education Policies and Guidelines. All students and staff are required to sign a Technology User Agreement that signify their understanding and promise to follow these regulations.

SCOPE OF COVERAGE FOR ALL TECHNOLOGY POLICIES

Policies, guidelines and rules described in this guide refer to all computing devices (including but not limited to computers, handhelds or PDAs, MP3 players, ipods, portable memory storage devices, calculators with interfacing capability, cell phones, digital cameras, etc.), technology infrastructure, associated peripheral devices and/or software:

- Owned by, leased by and/or on loan to The Cresskill Public School District.
- Owned by, leased by and/or on loan to any third party engaged in providing services for Cresskill Local Schools
- Any computing or telecommunication devices owned by, in the possession of or being used by district students and/or staff that are operated on the grounds of any district facility or connected to any equipment at any district facility by means of direct connection, telephone line or other common carrier or any type of connection including both hardwired, fiber, infrared and/or wireless.

PERSONAL RESPONSIBILITY

Students agree to not only following the rules in this policy, but are agreeing to report any misuse of any computer system to the person designated by the school for such reporting. Misuse means any violations of this policy or any other use that is not included in the policy, but has the effect of harming another or his or her property.

Rules for Computer and Network Use

1. **Do-** Follow all rules in the [AUP summarized](#) below.
2. **Do-** Ask a teacher or staff member when unsure of how to do something or you have a problem.
3. **Do-** Remember computer use is a privilege. Violation of rules can result in loss of computer privileges and/or other disciplinary action.
4. **Do not-** Remove or Add any programs or files to computers.
5. **Do not-** Change system settings.

6. **Do not-** Change Internet Browser settings.
7. **Do not-** Unplug cables or open computer cases.
8. **Do not-** Have any food, beverage near computers.
9. **Do not-** Force disks or CDs into or out of drives.
10. **Do not-** Visit inappropriate Internet sites.
11. **Do not-** Download programs from the Internet.
12. **Do not-** Attempt to learn or steal other's passwords or access unauthorized systems.
13. **Do not-** Use any "hacking" software. Possession of and/or distribution of any software tools designed to facilitate hacking or compromise a computer or network will also be considered an offense.
14. **Do not-** Waste paper and toner by printing the same page multiple times.
15. **Do not-** Bring viruses, spyware or other malware to our computers.
16. **Do not-** Send Messages across the network or use any instant messaging software/service.
17. **No-** "Roughhousing" around computer equipment
18. **Do not-** Violate any other building or classroom student rules during the use of computer technology.

ACCEPTABLE USE & INTERNET SAFETY POLICY (AUP)

ACCEPTABLE USES

Educational Purposes- The district provides access to its computer resources and the Internet for educational purposes. If you have any doubt about whether a contemplated activity meets this educational purpose, please consult with your classroom teacher and/or responsible staff member. Among the uses* that are considered acceptable include but are not limited to the following:

- A. Class work, utilizing technology, assigned and supervised by a staff member
- B. Class work, utilizing technology, specifically assigned but independently conducted
- C. Research for Educational Purposes
- D. Completion of Assignments for other classes
- E. Use of District provided software to enhance and/or reinforce student learning
- F. Training or Development of Computer Use Skills
- G. Personal Discovery of an acceptable nature ("surfing the Internet")

UNACCEPTABLE USES

Among the uses that are considered unacceptable include but are not limited to the following:

- A. Uses that violate any of the Computer Rules listed in the section above
- B. Uses that violate or encourage others to violate the law.
- C. Viewing, transmitting or downloading pornographic, obscene, vulgar and/or indecent materials or offensive or harassing messages.
- D. Intrude into networks or computers of others
- E. Uses that violate Copyright laws.
- F. Uses that cause harm to others or damage to their property. For example, don't engage in defamation (harming another's reputation by lies or hearsay)
- G. Uses that jeopardize individual computers, the network or user account security. For example, don't disclose or share your password with others.
- H. Uses that contribute to the violation of any other student conduct code including but not limited to: cheating, plagiarism, hazing or harassment, theft, falsification of records, possession of banned substances/items, etc.
- I. Uses that are designed to establish a commercial enterprise or provide system resources to an outside third party (including but not limited to: proxy server, remote access, file transfer, file sharing or storage)

capability, etc.)

- J. **“Hacking” and Other Illegal Activities.** Use of computer resources to attempt to gain unauthorized access to other computers, files or networks. Upload a worm, virus, Trojan, “time bomb” or any other harmful form of programming or malware, bypass filters, install any type of server, proxy, aliasing/spoofing peer-to-peer networking or remote-control software (including but not limited to: “Napster like programs”, Grokster, Limewire, BackOrifice, VNC, etc.). Possession of and/or distribution of any of the above software tools designed to facilitate any of the above actions will also be considered an offense.

INTERNET SAFETY

- A. **Individual Responsibility-** Users/parents/guardians are advised that use of any network includes the potential for accessing web sites with inappropriate materials. It is the responsibility of all users to attempt to avoid these sites through prudent use of the Internet. If a student accidentally accesses one of these sites, they should immediately exit from that site and/or notify a staff member. If a student finds that other users are visiting offensive or harmful sites, they should report such use to the proper authorities. Parents wishing to not have their children utilize district computers and/or the Internet must provide a written request to the Principal of their school, detailing the specific desired limitations.
- B. **Practice Personal Safety.** Do not reveal personal information such as your full name, home address, phone or credit card numbers or other information, which might allow a person to locate you. Do not arrange a face-to-face meeting with someone you “meet” on the Internet without your parent’s permission (if you are under 18). Avoid the use of web sites that allow you to share such private information about you, your family and/or friends with others.
- C. **Learn Tips for Safe Use of the Internet.** Parents are encouraged to visit with their students sites that are designed to teach safe Internet use.
- D. **Confidentiality of Student Information.** Personally identifiable student information may not be disclosed or used in any way on the Internet without the permission of a parent or guardian or a student who is 18 or older. A supervising teacher or administrator may authorize the release of directory information, as defined by Ohio law, for internal administrative purposes or approved educational activities.
- E. **Active Restriction Measures.** The District, either by itself or in combination with the provider of Internet access, will utilize filtering software or other technologies, in compliance with the Child Internet Protection Act of 2000, to prevent students from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors*. The District also reserves the right to monitor students’ computer/online activities, through direct observation and/or technological means, to ensure that students are not accessing such depictions or other such materials. It is important to note that any filtering system is not 100% effective, thus students should follow all district guidelines to avoid inappropriate web sites.

*The term “harmful to minors” is defined by the Communications Act of 1934 (47 USC Section 254 (h) (7)), as meaning any picture, image, graphic image file, or other visual depiction that: a. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion; b. depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; c. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

PRIVACY

The District reserves the right to monitor, inspect, copy, review and/or store at any time and without prior notice any and all results of usage of computers, network and/or Internet access and any and all information transmitted or received in connection with such usage. All such information shall be and remain the property of the District and users shall have no expectation of privacy regarding such materials.

FAILURE TO FOLLOW POLICY

Use of the computer network and Internet is a privilege, not a right. Policy violators shall be dealt with following

established student discipline guidelines. The district also reserves the right to limit, temporarily or permanently, use of computer resources, or a subset of these resources, by any student involved in an infraction that involves the use of computer resources. Any infractions that fall under the provisions of the New Jersey and Federal Criminal Codes will be referred to the appropriate law enforcement agencies.

WARRANTIES / INDEMINIFICATION

The Cresskill School District makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this policy. It shall not be responsible for any claims, losses, damages or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user's use of its computer networks or the Internet under this policy. By agreeing to this policy, users are taking full responsibility for his or her use, and the user who is 18 or older, or in the case of a user under 18, the parent(s) or guardian(s) are agreeing to indemnify and hold the school, the school district, the ITC or ISP that provides the computer and Internet access opportunity to the school district and all of their administrators, teachers, and staff harmless from any and all loss, costs, claims or damages resulting from their user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s) or guardian(s) agree to cooperate with the school in the event of the school's initiating an investigation of a user's use of his or her access to its computer network and the Internet, whether that use is on a school computer or on another computer outside the Cresskill School District's network.

POLICY UPDATES

Due to the rapidly changing nature of technology, updates to this policy will be posted on the official site of the Cresskill Public School District and these updates will supersede or amend the rules as stated within any printed document.