

# Arcadia Local School



## Acceptable Use & Internet Safety Policy

## **Arcadia Local Schools Acceptable Use and Internet Safety Policy**

It is the intention of the Arcadia Local Board of Education to protect the privacy of students who use the school computers, computer network, and electronic messaging systems to the maximum extent possible given the operational and security needs of the District.

The purpose of this policy is to identify the limitations on this privacy and the general restrictions applying to the use of computers and electronic messaging systems of the District.

### ***Acceptable and Unacceptable Uses***

The use of Technology in the Arcadia School District is an opportunity extended to students, faculty, and staff to enhance learning, productivity, and information processing. The computers, computer network, and internet shall be used solely for educational purposes specified by the Arcadia Board of Education and the faculty of the School District.

### **The following are uses which are unacceptable under any circumstances:**

- the transmission of any language or images which are of a graphic sexual nature
- the transmission of jokes, pictures, or other materials which are obscene, lewd, vulgar, or disparaging of persons based on their race, color, sex, age, religion, national origin, or sexual orientation the transmission of messages or any other content which would be perceived by a reasonable person to be harassing or threatening uses that constitute defamation (libel or slander)
- uses that violate copyright, trademark, patent and/or protected intellectual property rights and/or laws
- “hacking” uses that attempt to gain unauthorized access to another computer system and/ or organizational or personal data information filed or to impair the operation of another computer system (for example, the transmission of a computer virus or an excessively large e-mail attachment)
- any commercial or profit-making activities
- any fundraising activities, unless specifically authorized by an administrator
- installation of any personal hardware or software
- removal or relocation of any district computer hardware without the explicit permission of the Technology Coordinator or building administrator
- attempts to circumvent the Internet filter
- attempts to connect non district hardware to the computer network
- Any act that violates Public Law 107-110 Section 2441, No Child Left Behind

### ***Security and Integrity***

Students shall not take any action which would compromise the security of any computer, network or messaging system. This would include the unauthorized release or sharing of passwords and the intentional disabling of any security features of the system.

Students shall not take any actions which may adversely affect the integrity, functionality, or reliability of any computer (for example, the installation of hardware or software not authorized by the Technology Coordinator). Students shall report to the Technology Coordinator or a School District administrator any actions by students which would violate the security or integrity of any computer, network or messaging system whenever such actions become known to them in the normal course of their educational experience.

## *Internet Safety*

- **General Warning; Individual Responsibility of Parents and Users.** All users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged pupils. Every user must take responsibility for his or her use of the computer network and Internet and stay away from these sites. Parents of minors are the best guide to materials to shun. If a student finds that other users are visiting offensive or harmful sites, he or she should report such use to the person designated by the School.
- **Personal Safety.** Be safe. In using the computer network and Internet, do not reveal personal information such as your home address or telephone number. Do not use your real last name or any other information which might allow a person to locate you without first obtaining the permission of a supervising teacher. Do not arrange a face-to-face meeting with someone you “meet” on the computer network or Internet without your parent’s permission (if you are under 18). Regardless of your age, you should never agree to meet a person you have only communicated with on the Internet in a secluded place or in a private setting.
- **Safety and Security.** The Superintendent shall prepare guidelines that address students’ safety and security while using internet services. Building principals are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying guidelines. The board expects that staff members will provide guidance and instruction to students in the appropriate use of the Internet. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response. All internet users (and their parents if they are minors) are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines
- **“Hacking” and Other Illegal Activities.** It is a violation of this Policy to use the School’s computer network or the Internet to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.
- **Confidentiality of Student Information.** Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian or, if the student is 18 or over, the permission of the student himself/herself. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and Social Security numbers. A supervising teacher or administrator may authorize the release of directory information, as defined by Ohio law, for internal administrative purposes or approved educational projects and activities.
- **Active Restriction Measures.** The School, either by itself or in combination with the Data Acquisition Site providing Internet access, will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors. The School will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material which is inappropriate for minors.
- **Internet filtering software** or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects.

- 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
  - taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
  - 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;
  - Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

### ***Right of Access***

Although the Arcadia Board of Education respects the natural desire of all persons for privacy in their personal communications, and will attempt to preserve this privacy whenever possible, the operational and security needs of the District’s computer network and messaging systems require that full access be available at all times. The School District therefore reserves the right to access and inspect any computer, device, or electronic media within its systems and any data, information, or messages which may be contained therein. All such data, information, and messages are the property of the School District and students should have no expectation that any messages sent or received on the School District’s systems will always remain private.

### ***Signed User Agreement***

Annually, a student who wishes to have computer network and Internet access during the school year must read the acceptable use and Internet safety policy and submit a properly signed agreement form. Staff members are asked to sign a new agreement each year after reviewing the policies and regulations of the District. A user’s agreement is signed to indicate the user’s acknowledgment of the risks and regulations for computer/on-line services use. Employees, students and parents of students must be aware that the privileges to access on-line services are withdrawn from users who do not respect the rights of others or who do not follow the rules and regulations established.

# Arcadia Local School Network Usage Agreement

## Students' Network Usage Agreement

By signing this Policy and Agreement, you are agreeing not only to follow the rules in this Policy and Agreement, but also agreeing to report any misuse of the network to the person designated by the School for such reporting. Misuse means any violations of the Policy or any other use that is not included in the Policy, but has the effect of harming another or his or her property.

I have read, understand and agree to abide by the terms of the foregoing Acceptable Use Policy and Agreement. Should I commit any violation or in any way misuse my access to the School District's computer network and the Internet, I understand and agree that my access privilege may be revoked and School disciplinary action may be taken against me.

Student's grade level: \_\_\_\_\_

---

_____ User's Signature	_____ Date	_____ Name (Print clearly)	_____ Phone
---------------------------	---------------	-------------------------------	----------------

---

Address

## Parent or Guardian Network Usage Agreement

As the parent or legal guardian of this student, I have read, understand and agree that my child or ward shall comply with the terms of the District's Acceptable Use Policy and Agreement for the students' access to the School District's computer network and the Internet. I understand that access is being provided to the student for educational purposes only. However, I also understand that it is impossible for the School to restrict access to all offensive and controversial materials and understand my child's or ward's responsibility for abiding by the Policy and Agreement. I am therefore signing this Policy Agreement and agree to indemnify and hold harmless the school, the School District and the Data Acquisition Site that provides the opportunity to the School District for computer network and Internet access against all claims, damages, losses and costs, or whatever kind, that may result from my child's or ward's use of his or her access to such networks or his or her violation of the foregoing Policy and agreement. Further, I accept full responsibility for supervision of my child's or ward's use of his her access account if and when such access is not in the school setting. Please check and complete one of the two sections below.

---

_____ Parent/Guardian (Signature)	_____ Date	_____ Parent/Guardian (Please Print)	_____ Phone
--------------------------------------	---------------	---	----------------