File: IJNDB

ERVING ELEMENTARY SCHOOL
ACCEPTABLE USE POLICY (AUP)

The AUP provides parents/guardians, students, staff, community members, and guest users, with a statement of purpose and explanation of the use of technology within the learning community. This procedure is reinforced by instruction, practice, responsible use guidelines and is required to be read before accessing the technology devices, digital resources, and network infrastructure. Students, parents/guardians, staff and community members must also read and sign the accompanying Statement of Responsibilities. We respect each family's decision whether their child should or should not have access to the Internet. Students will be given an account on the network and access to the Internet only if a parent or legal guardian submits a signed Acceptable Use Form. Once agreed to, access to electronic resources will remain in force for the duration of the student's enrollment, staff employment or community member's active residential status unless expired, or revoked due to violations of this policy.

These guidelines are based on the Children's Internet Protection Act (CIPA) and its four guiding principles of respect, privacy, sharing, and safety. These guidelines are appropriate for all technology users. Every user has the responsibility to respect and protect the rights of every other user in our school communities and on the Internet. Account holders are expected to conduct themselves in a responsible, ethical, and legal manner, consistent with the school and district policies, rules, regulations and guidelines and the laws of the Commonwealth of Massachusetts and the United States.

Erving Elementary School (EES) provides access to electronic resources that promote educational excellence, information sharing, innovative instruction and online communication. All users are encouraged to use electronic devices, the computer network and the Internet to pursue intellectual activities, seek resources, access libraries, collaborate and engage in learning activities. Online communication constitutes but is not limited to email, Internet, blogging and any use of network resources. EES electronic resources include, but are not limited to, all hardware, software, data, communication devices, printers, servers, filtered Internet access, and local and wide area networks.

Online communication is critical for today's learners to apply 21st Century Skills and employs tools such as interactive websites, blogs, video conferencing, and podcasts which offer authentic opportunities for students to express and share information.

This AUP outlines the rules and guidelines under which all members of the EES community (students, staff, guests and community) will be held accountable.

In all cases it is the responsibility of parents/guardians, students, staff and community members to immediately report any findings of improprieties to school administration.

RESPONSIBLE USE GUIDELINES

EES has established protocols to ensure the safety of our school community, the security of computer networks, and compliance with applicable law. All users should be aware of the following standard practices:

Content Filtering

The Erving Elementary School uses software designed to block access to certain sites and filter content as required by the Children's Internet Protection Act, 47 U.S.C. §254 (CIPA). EES is aware that not all inappropriate information can be filtered, and the district will make a concerted and ongoing effort to correct any known gaps in the filtering of information without unduly inhibiting the educational use of age appropriate content by staff and students. Users will inform teachers or administrators of any inadvertent access to inappropriate material, in order that there is appropriate modification of the filtering profile. EES will educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms as well as cyberbullying awareness and response.

Student Safety. To ensure personal safety and the safety of others, users shall not publish or send any message that includes personal information such as home address, personal phone numbers and/or last name for any individual student. The staff is not permitted to post this information to public domains (i.e. class web page or Internet). Student pictures and/or work may only be included on district/ school/ classroom websites with parent/guardian permission and without identifying captions unless the site is password protected.

All users are expected to exercise care when using technology equipment/resources and to follow directions for proper use. Any user whose action alters the proper functioning of equipment may face disciplinary action and may be charged for the repair or replacement of the equipment.

Student use of electronic resources is restricted to teacher-approved projects and research. Student use of the Internet will be under the supervision of school staff, but due to the nature of the Internet and evolving technology, students might get to an inappropriate site inadvertently. It is the student's responsibility to immediately report any inappropriate site to a staff member.

Teachers of K-2 students will establish access to appropriate student websites via the use of personalized learning environments (i.e. pathfinders, classroom webpages). Students in grades 3-6 may not attempt to access any Internet resource without the prior consent and only with direct supervision of staff.

Password Protection. Passwords are provided for each user's personal use only and are, therefore, confidential. Passwords should never be shared, stolen or used by another person. If a student or staff member suspects that a password has been compromised, they should notify a teacher or network administrator. Student usernames and passwords will be established and assigned by the network administrator. Staff usernames will adhere to established naming conventions.

Privacy. Students and staff need to be aware that files stored on school computers are not private. Network and internet access is provided as a tool for educational purposes only. The District has the right to monitor, inspect, copy, review and store any and all usage of the computer network and Internet access, including transmitted and received information, without prior notice. All information files are the property of the District and no user shall

have any expectation of privacy regarding such files. Federal Law requires that all email, sent and received, be stored for a period of seven years. The District may choose to archive longer.

Online Etiquette. All school users are expected to use appropriate language and graphics, and shall not engage in swearing, vulgarities, suggestive, obscene, belligerent, harassing, threatening or abusive language of any kind. School online access may not be used to make, distribute, or redistribute cyber bullying, obscene material or material which is based on slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, gender identity or sexual orientation.

Messaging. Teachers may incorporate restricted email, protected blogs, podcasts, video conferencing, online collaborations, electronic devices, instant messaging, texting, tweeting, walled garden social media, Virtual Learning Environments and other forms of direct electronic communications or internet applications for educational purposes. Although teachers monitor student online activity, it is the direct responsibility of the user to comply with this AUP.

Internet Tools. Use of blogs, podcasts, or other internet tools are considered an extension of the classroom. Whether at home or in school, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other internet tools. Students using blogs, podcasts or other internet tools are expected to act safely and responsibly by keeping all personal information out of their posts. Comments made on school related blogs should follow the rules of online etiquette detailed above and will be monitored by school personnel. If inappropriate, they will be deleted. Users must not link to websites from a blog without reading the entire article to make sure it is appropriate for a school setting.

General Communications Guidelines

Below is a general summary of guidelines related to email and any form of online chat or instant messages. Email and online chat is to be used for school related communication.

The following practices are not allowed when using EES resources:

- Sending harassing email or instant messages or content.
- Sending offensive email or instant messages or content.
- Sending spam email or instant messages or content.
- Sending email or instant messages containing a virus or other malicious content.
- Sending or reading email or instant messages at inappropriate times, such as during class instruction.
- Sending email or instant messages to share test answers or promote cheating in any way.
- Using the account of another person.

Plagiarism/Copyright/Licensing. Plagiarism is the act of using someone else's words or ideas as your own. Students and staff are required to give proper credit to all Internet and non-electronic sources used in academic assignments, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music, and text. Plagiarism of Internet and non-electronic resources will be addressed in a developmentally appropriate manner. In addition, all students and staff must adhere to the copyright laws of the United States (P.L.94553) and the Congressional Guidelines that delineate it regarding software,

authorship, and copying information. All students and staff must adhere to the Creative Commons licenses where the author/artist denotes what media may be shared, remixed, or reused.

Proxies. The use of anonymous proxies to avoid content filtering is strictly prohibited and is a direct violation of this agreement.

Illegal Activity. Use of any EES electronic devices/resources for any illegal activity is prohibited. Illegal activities include but are not limited to:

(a) tampering with computer hardware or software,
(b) software piracy
(c) unauthorized entry into computers and files (hacking),
(d) knowledgeable vandalism or destruction of equipment,
(e) deletion of computer files belonging to someone other than oneself,
(f) uploading or creating of computer viruses,
(g) distribution of obscene or pornographic materials,
(h) sexting and
(i) cyberbullying

Such activity is considered a crime under state and federal law. Users must be aware that any illegal action carried out over the Internet will be reported to law enforcement officials for possible prosecution. Please be advised it is a federal offense (felony) to break into any security system. Financial and legal consequences of such actions are the responsibility of the user (staff, guests, and student) and student's parent or guardian.

Cyberbullying. The use of electronic devices, digital resources and the network for the purpose of cyberbullying is strictly prohibited both on and off school grounds.

Cyberbullying as defined by Chapter 92 of the Acts of 2010 (An Act Relative to Bullying in Schools) is bullying through the use of technology or any electronic communication, which shall include, but shall not be limited to, any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system, including, but not limited to, electronic mail, Internet communications, instant messages or facsimile communications. Cyberbullying shall also include (i) the creation of a web page or blog in which the creator assumes the identity of another person or (ii) the knowing impersonation of another person as the author of posted content or messages, if the creation or impersonation creates any of the conditions enumerated in clauses (i) to (v), inclusive, of the definition of bullying. Cyberbullying shall also include the distribution by electronic means of a communication to more than one person or the posting of material on an electronic medium that may be accessed by one or more persons, if the distribution or posting creates any of the conditions enumerated in clauses (i) to (v), inclusive, of the definition of bullying.

TERMS OF AGREEMENT

Erving Elementary School reserves the right to deny, revoke or suspend specific user privileges and/or to take other disciplinary action, up to and including suspension, expulsion (students), or dismissal (staff) for violations of these Guidelines. The District will advise appropriate law enforcement agencies of illegal activities conducted through the EES Internet connection. The District also will cooperate fully with local, state, and/or federal officials in any investigation related to any illegal activities conducted through the network. The school district and their representatives are not responsible for the actions of the users or the information they access.