

# ESCANABA AREA PUBLIC SCHOOLS

## *Acceptable Use Policy*

*Revised January, 2009*

### *Guidelines for the acceptable use of the EAPS Computer Network*

The intent of this document is to provide students and staff, hereafter known as **Users**, with the information necessary to comply with all guidelines approved by the Escanaba Area Public School District, hereafter known as the **District**, when using District-owned computer hardware or software resources, hereafter known as the **Computer Network**. Unless amended by the District, the provisions contained within this document will be in effect for the duration that the User remains with the District.

Pursuant to section 6 of the Michigan Library Privacy Act, each school library offering public access to the Internet or a computer, computer program, computer network, or computer system shall limit minors to only use, or view those using, terminals that do not receive obscene material or sexually explicit matter that is harmful to minors. Individuals age 18 or older, or a minor accompanied by their parent/guardian, may access a school library terminal that is not restricted from receiving such materials. The building principal shall designate the individual responsible for implementing this policy in each qualifying school building library.

In accordance with the Children's Internet Protection Act, the District has implemented this policy, in part, to:

- promote the safe, ethical, responsible, and legal use of the Internet;
- support the effective use of the Internet for educational purposes;
- protect students against potential dangers in their use of the Internet; and
- ensure accountability.

The District provides and maintains a Computer Network for the benefit of all Users. Users are encouraged to use and enjoy the Computer Network to enhance their educational experience. Users are responsible for good behavior while using the Computer Network—just as would be expected in other areas of the school building. Users should remember that access to the Computer Network is a privilege, not a right.

The District's Computer Network is intended for educational purposes and District business and is neither a public access service nor a public forum. Only District students and staff who agree to the terms of this policy may be granted access to the District's Computer Network.

In exchange for the use of the District's Computer Network, I, the undersigned, understand and agree to the following conditions:

#### **1. User's Responsibilities**

- a. All information, services, and features contained on the Computer Network are intended for use solely by registered Users, only to facilitate learning and enhance information exchange consistent with legitimate educational and work-related purposes. Any use of these resources for commercial, for-profit, or any other unauthorized purposes (i.e. advertisements, political lobbying, marketing), in any form, is expressly forbidden. The District's Network shall not be used to:
  - i. Post or disclose personal identification information about yourself or others over the Internet, even if this information is solicited by a web site that requests such information.
  - ii. Advertise, offer, or provide goods or services for financial gain.
  - iii. Lobby politicians; although Users may communicate opinions with elected governmental representatives.
  - iv. Draft, send or receive inappropriate materials or to engage in behavior which violates District policy, (Including the student conduct code) or which violate federal, state, or local law or regulation. Users are directly responsible for the safekeeping of their unique user ID and password. Any problems that arise from the use of a User's account are the sole responsibility of the account holder. Use of an account by someone other than the registered User is forbidden and is grounds for loss of access to the Computer Network.
- b. It is the responsibility of the User to report, to their supervisor or instructor, any and all damage that may have occurred while they were using any District-owned equipment.
- c. Should a User willfully transfer/download a file or software that infects the Computer Network and/or causes malicious damage, the User will be directly liable for any and all costs to repair the Network. Additionally, the User may be subject to other disciplinary measures as determined by the District.
- d. It is the responsibility of the User when connecting a removable media device, including USB Flash Memory devices, to the Computer Network to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied when using the removable device. It is imperative that any portable memory devices be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that User's account. Users will follow normal data removal procedures to permanently erase District data from such devices once their use is no longer required.
- e. Users have no expectation of privacy as to information or activity on the District's Computer Network. Misuse of a User's account may result in suspension of the account privileges and/or disciplinary action as determined by the District. Misuse shall include, but is not limited to:
  - i. Attempting to connect and/or use personal hardware and/or software on the District's Computer Network, without the express permission of the District.
  - ii. Use of web-based or anonymous proxy servers to bypass or circumvent District Internet filtering devices.
  - iii. Use of personal wireless devices, such as cell phones or handheld video games, that attempt to connect to, or disrupt, the District's wireless infrastructure.

- iv. Disrupting the operation of the Computer Network through abuse of the hardware or software of any component of the Network, including personal computers.
  - v. Intentionally seeking information on, obtaining copies of, or modifying files, other data, or passwords belonging to other Users.
  - vi. Malicious use of the Computer Network through harassment, profanity, vulgar statements or discriminatory remarks.
  - vii. Downloading or installing unauthorized software, or the unauthorized modification, copying, or use of licensed or copyrighted software.
- f. Users are expected to:
- i. Seek instruction for the use of any available technology for which the User is not familiar.
  - ii. Attend appropriate training sessions in the use and care of hardware, software, and network peripherals.
  - iii. Student use of e-mail, chat, instant messaging, and other forms of two-way electronic communications shall only be for legitimate educational purposes and only under the direct supervision of an adult.
  - iv. Promptly notify an instructor or supervisor about any electronic message you receive that is inappropriate or makes you feel uncomfortable.
  - v. Maintain the integrity of the electronic messaging systems by deleting files/messages which have exceeded their established limit and by reporting any security violations.
  - vi. Keep inappropriate material from entering the Computer Network or from being reproduced in visual, digital, or written format.
  - vii. Comply with all applicable state and federal laws, including copyright, trademark laws, and applicable licensing agreements, in using the District's electronic information technologies.

## 2. District's Rights

- a. The District reserves all rights to any and all electronic data stored on its Computer Network, including, but not limited to, District file servers. The District reserves the right to electronically monitor the movement of data across its Computer Network. The District may periodically make determinations on whether specific uses of the network are consistent with the Acceptable Use Policy. The District reserves the right to monitor and log Internet use, user activity, and file server space utilization by the User. When deemed necessary, the District also reserves the right to deny any User access to its Computer Network in an effort to prevent further unauthorized activity.
- b. The District utilizes Internet filtering software that is intended to block access to materials that are unlawful, obscene, pornographic, offensive, or otherwise objectionable. The District does not guarantee that school officials can control access to all such materials, or that users will not have access to such materials while using the Computer Network. The District can and will remove any and all material which the District, at its sole discretion, believes may be unlawful, obscene, pornographic, offensive, or otherwise objectionable. Users will not use the Computer Network to obtain, view, download, print, or otherwise gain access to such materials.
- c. The District does not warrant that the functions of its Computer Network will meet any specific requirements that the User might have, or that it will be error-free or uninterrupted; nor shall it be liable for any indirect, incidental, or consequential damages (including lost data, information, or time) sustained or incurred in connection with the use, operation, or inability to use the system. In consideration for the privileges of using the Computer Network, and in consideration for having access to the information contained therein, the User hereby releases the District from any and all claims of any nature arising from use, or inability to use, its Computer Network.
- d. The District reserves the right to refuse, by physical and non-physical means, the ability for the User to connect removable media, including USB Flash Memory devices, to its Computer Network and will engage in such action if it feels such equipment is being used in such a way that puts the Computer Network at risk.
- e. In the event of improper use of its Computer Network, the District reserves the right to remove files, limit or deny access, and/or refer Users for other appropriate disciplinary actions. The District reserves the right to revoke the User's access privileges immediately and without warning.

### Policy Definitions:

**Educational purposes** include but are not limited to the use of the District's Computer Network for classroom activities, continuing education, professional or career development, and high-quality, educationally enriching personal research.

**Harmful to minors** means "any picture, image, graphic image file, or other visual depiction that (1) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (2) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act of sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (3) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors." 47 USC 254 (h)(7)

**Inappropriate material** includes but is not limited to materials that are harmful or inappropriate to minors, obscene, pornographic, profane, vulgar, harassing, threatening, defamatory, or otherwise prohibited by law. The determination of a materials' "appropriateness" is based on both the material's content and intended use.

**Vandalism** is any attempt to harm, destroy, disrupt, or hack the operation of the District's electronic informational technologies, including but not limited to the creation or intentional receipt or transmission of computer viruses.

**Please sign and return this portion of the Acceptable Use Policy to receive your account information.**

*I agree to abide by such rules and regulations of the District's Computer Network usage as outlined in the Acceptable Use Policy. I also agree that I will reimburse the District for any fees, expenses, or damage incurred as a result of my use or misuse of its Computer Network.*

\_\_\_\_\_  
Signature of Student/Staff

\_\_\_\_\_  
Date

\_\_\_\_\_  
Please legibly print the student's/staff name here

\_\_\_\_\_  
Building

*I will instruct my child about any other access restrictions in addition to those set forth in District Policy. I will emphasize to my child the importance of following the District rules for personal safety.*

\_\_\_\_\_  
Signature of Parent/Guardian

\_\_\_\_\_  
Date