TECHNOLOGY ACCEPTABLE USE/EMPLOYEE CODE OF CONDUCT
SCHOOL DISTRICT OF ALTOONA

Overview

Employees who use School District of Altoona (the "District") computer and network facilities assume responsibility for their appropriate use. The District expects employees to be careful, honest, and responsible in their use of school technology. The computers, software, electronic and network resources are owned by the District and are provided to support employees in the execution of their job duties. All internet and email communications are public and not private in nature. As such, the District reserves the right to monitor and access an employee's internet activities and email content.

Some personal use of school district technology is permitted so long as the following conditions are met: such use shall not interfere with the employee's job performance, shall not violate any rules contained in any school district policy, or any state or Federal law, and shall not damage the District's hardware, software or communications systems including use that degrades or disrupts network performance.

Use of district technology resources for commercial or political activities or for financial gain is prohibited unless there is a clear and definable educational purpose. Computers shall not be used to view or disseminate sexually explicit, vulgar, indecent, obscene, offensive, lewd, or harassing communications to other individuals or organizations. Employees shall be aware that criminal sanctions are provided under Wis. Stat. 947.0125 for threatening, intimidating, abusive, or harassing messages sent to another person through electronic mail or other computerized communication systems.

Users shall not access another user's account without permission. Passwords are confidential and must not be shared with anyone. Users should give careful consideration before disclosing personal identification information about themselves to online entities or organizations. No unauthorized disclosure of student personal identification information is permitted.

The District will not be held liable for information that may become lost, damaged, or unavailable due to technical or other difficulties. The District is not liable for losses, claims, or demands against the District or any user by any other party based on the user's unethical or illegal use of technology resources. Users may discover controversial materials that do not further the purposes of education and research. It is the user's responsibility not to initiate access to such materials. It is not possible for the District to always prevent this from occurring. Users must be attentive to and adhere their use of the District's technology resources to gain access to materials with educational value. Furthermore, the District cannot guarantee that persons using the system will not be exposed to controversial materials. Such exposure is possible and is beyond the control of the District.

Internet and Electronic Communications

See the attached Internet Safety Policy for additional information regarding Internet and email use and CIPA and NCIPA.

Employees using the Internet and electronic communications technologies provided by the District must follow general professional rules for behavior and communication. All Internet and email correspondence is public and not private. The District reserves the right to monitor, access and disclose an employee's Internet activities and email content without notification or permission. Internet filters are required on all district computers. Filters may be temporarily disabled only when there is a clear and definable educational purpose. Careful consideration must be given to email attachments because of virus threats. Attachments should only be opened when the attachment is required for job performance

Network Storage

Many employees are provided with file server storage spaces. Using the file server is highly recommended and is a convenient and safe place to store documents and files. Employees should be aware that server space is limited. Staff should periodically delete files that are no longer needed. Files that need to be kept, but are no longer accessed can be burned onto a CD for archiving and then deleted from the server. Users will not store files or software on the server when doing so is in violation of copyright. When in doubt as to copyright status of files or software to be stored, the user should contact the Library Media Specialist in his/her building for help in determining its copyright status before storing them on the server.

Computer Hardware and Software

Computer hardware is provided to employees as a tool used in the carrying out of the employees' job duties. No hardware alterations shall be made to any District owned equipment without permission of the district Technology Coordinator. All software that is installed on district owned computers must, be legally licensed by the District. Employees shall not install software without the permission of the employee's building Library Media Specialist or the District's Technology Coordinator. It is the responsibility of the employee to regularly update the virus software loaded on the employee's computer.

Internet Safety Policy

Introduction

It is the policy of the School District of Altoona to (a) prevent user access over its computer network to, or transmission of, inappropriate material via the Internet, electronic mail, or other forms of electronic communications; (b) prevent unauthorized 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)].

Definitions

CIPA definitions of terms:

TECHNOLOGY PROTECTION MEASURE. The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

1. OBSCENE, as that term is defined in section 1460 of title 18, United States Code;

2. CHILD PORNOGRAPHY, as that term is defined in section 2256 of title 18, United States Code; or

3. Harmful to minors.

HARMFUL TO MINORS. The term "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 or 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.

SEXUAL ACT; SEXUAL CONTACT. The terms “sexual act” and “sexual contact” have the meanings given such terms in section 2246 of title 18, United States Code.

Access to Inappropriate Material

To the extent practicable, technology protection measures (or “Internet filters”) shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

Specifically, as required by the Children’s Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. No filtering technology is 100% effective in blocking all obscene, or “harmful” sites.

Subject to staff supervision, technology protection measures may be temporarily disabled only for bona fide research or other lawful purposes. Students shall not disable filtering technologies.

Inappropriate Network Usage

To the extent practicable, steps shall be taken to promote the safety and security of users of the School District of Altoona computer network when using electronic mail, and the Internet.

Specifically, as required by the Children’s Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called ‘hacking,’ and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Supervision and Monitoring

It shall be the responsibility of all members of the School District of Altoona staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children’s Internet Protection Act.

Users should consider all network activities public and not private. The District reserves the right to monitor, access and disclose a user’s network, Internet and email activities at any time without notification or permission.

Discipline and Penalties

In fulfilling the district's obligation to maintain a positive and productive work environment, the administration will make every attempt to correct any violations of this policy of which they become aware by calling attention to this policy or by more direct progressive disciplinary action, if necessary.

Violations of this policy, with respect to the use of District technology resources or a violation of state or federal law may result in a limitation of access privileges or their temporary or permanent loss. The District reserves the right to impose employment-related sanctions, including but not limited to oral or written warnings, suspensions or termination from employment. The District reserves the right, where it has deemed to be appropriate, to refer offenders to the appropriate authorities for violations of state or federal law. Under no circumstances shall any user be entitled to any expectation that his/her privilege of use shall not be suspended or revoked without first providing the user with an opportunity to be heard or to rectify his/her inappropriate use.

Initial Adoption: 07/21/03

Final Adoption: 08/04/03