Employee Technology Acceptable Use Policy

Section 1. Introduction. Computer information systems and networks are an integral part of business and instruction at East Allen County Schools. The corporation has made a substantial investment in human and financial resources to create these systems. Any District computer used by students shall have Internet filtering software in place either on the computer itself, or on the server through which the computer accesses the Internet.

The enclosed policies and directives have been established in order to:

1. Protect this investment.

2. Safeguard the information contained within these systems.

3. Reduce business, instructional and legal risk.

4. Protect the good name of the corporation.

Section 2. Violations. Violations and failure to comply with this policy by employees or students may result in disciplinary action up to and including discharge by the corporation depending upon the type and severity of the violation, whether it causes any liability, expense, or loss to the corporation, and the presence of repeated violation(s).

Section 3. Administration. The Director of Technology is responsible for the administration of this policy.

Section 4. Contents. The topics covered in this document include:

1. State of responsibility.

2. Software copyrights and license agreements.

3. The Internet and email.

4. Miscellaneous:

   A. Computer viruses

   B. Access codes and passwords

   C. Physical security

Section 5. Statement of General Responsibility. General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities:

1. Director of Technology Responsibilities. The Director of Technology must:

   A. Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with this policy.

   B. Provide appropriate support and guidance to assist employees to fulfill their responsibilities under this policy.

2. Building Level and Central Office Administrative Responsibilities. Building level and central office administrators must:

   A. Ensure that all appropriate personnel are aware of and comply with this policy.

   B. Create appropriate procedures to provide assurance that all employees observe this policy.

Section 6. Software Copyrights and License Agreements. It is East Allen County Schools' policy to comply with all laws regarding intellectual property.

1. Legal Reference: East Allen County Schools and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U.S. Code) and all proprietary software license agreements. Noncompliance might expose East Allen County Schools and the responsible employee(s) to civil and/or criminal penalties.

2. Scope: This policy applies to all software that is owned by East Allen County Schools, licensed to East Allen County Schools, or developed using East Allen County Schools' resources by employees or vendors.

3. Technology Department Responsibilities. The Director of Technology will:

   A. Maintain records of software licenses owned by East Allen County Schools;

B. Periodically (at least annually) scan company computers to verify that only authorized software is installed; and

C. Develop a database template specifying licensing information to be maintained and develop guidelines for establishing a storage facility.

4. Building Level Responsibilities. The designated software librarian will:

A. Be responsible for maintaining records of software licenses owned by East Allen County Schools but purchased by building level funds; and

B. Keep the media with the software license and documentation.

5. Employee Responsibilities. Employees shall not:

A. Install software unless approved, tested and supported by the Technology Department. Only software that is licensed to or owned by East Allen County Schools is to be installed on East Allen County Schools computers;

B. Copy software unless authorized by the copyright holder. (Note: Refer to http://www.eacs.k12.in.us/technology/software for a listing of software for which district site licensing is owned by EACS; and

C. Download software file types, such as exe, mp3, zip, unless authorized by the Technology Department. (Note: Prior to downloading software, check http://www.eacs.k12.in.us/technology/filetype for file types that should not be downloaded.

D. District staff shall not allow students to use any computer in the District with Internet capability that does not have Internet filtering software. This includes any computer, laptop or desktop, in the District's Libraries or media centers, classrooms, laboratories, or offices where students are, for any reason, allowed to use a computer, or any other such device, with Internet access.

6. Civil Penalties: Violations of copyright law expose the corporation and the responsible employee(s) to the following civil penalties:

   A. Liability for damages suffered by the copyright owner;

   B. Profits that are attributable to the copying; and

   C. Fines up to $100,000 for each illegal copy.

7. Criminal Penalties: Violations of copyright law that are committed "willfully and for purposes of commercial advantage or private financial gain (Title 18, Section 2319(b)" expose the corporation and the employees responsible to the following criminal penalties:

   A. Fines up to $250,000 for each illegal copy; and

   B. Jail terms of up to five (5) years.

Section 7. The Internet and Email. The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide. One popular feature of the Internet is email.

1. Policy: Access to the Internet is provided to employees for the benefit of East Allen County Schools, its students and staff. Employees are able to connect to a variety of information resources around the world.

   Conversely, the Internet is also replete with risks and inappropriate material. To ensure that all employees are responsible and productive Internet users and to protect the corporation's interests, the following rules have been established for using the Internet and email.

   A. Acceptable Use: Employees using the Internet are representing the school corporation. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

      i. Using Web browsers to obtain business/educational information from commercial Web sites;

      ii. Using the Internet as a research tool;

iii. Accessing databases for information as needed; and

iv. Using email for professional contacts.

B. Unacceptable Use: Employees must not use the Internet for purposes that are illegal, unethical, immoral, harmful to the corporation, or nonproductive. Examples of unacceptable use are:

i. Sending or forwarding chain email, i.e. messages containing instruction to forward the message to others;

ii. Indiscriminate broadcasting email, i.e. sending the same message to a large number of people regardless of the relevance of the message to those people;

iii. Conducting a commercial business using corporation resources;

iv. Viewing, sending, or receiving pornography or any other obscene material;

v. Transmitting any content that is offensive, harassing, or fraudulent;

vi. Playing video games; and

vii. Non-instruction use of streaming audio.

2. Downloads: File downloads from the Internet are not permitted unless the file type is specifically authorized by the Director of Technology.

3. Employee Responsibilities: An employee who uses the Internet and/or email shall:

A. Use the electronic mail system primarily for the conducting of corporation business; however personal use on an occasional basis to communicate with family, friends, and others is permissible as long as it does not substantially or materially interfere with the employee's productivity.

B. Be responsible for the content of all text, audio, or images that (s)he places or sends over the Intranet or Internet. All communications shall have the employee's name attached.

D. Not transmit copyrighted materials without permission.

D. Know and abide by all applicable East Allen County Schools' policies dealing with security and confidentiality of corporation records.

E. Run a virus scan on any executable file(s) received through the Internet.

F. Avoid transmission of nonpublic corporation information. If it is necessary to transmit nonpublic information, employees are required to take steps reasonably intended to ensure that this information is delivered to the proper person who is authorized to receive such information for a legitimate use.

4. Copyrights: Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the corporation and/or legal action by the copyright owner.

5. Monitoring. All messages created, sent, or retrieved over the East Allen County Schools mail system or the Internet are the property of the corporation**.** East Allen County Schools reserves the right to access the contents of any messages sent over its facilities if the corporation believes, in its sole judgment, that it has a need to do so.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

Section 8. Miscellaneous.

1. Computer viruses: Computer viruses are programs designed to make unauthorized changes to programs and data; therefore, viruses can cause destruction of corporate resources. It is important to know that (1) computer viruses are much easier to

prevent than to cure; and (2) defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

2. Technology Department Responsibilities: The Technology Department shall:

   A. Install and maintain appropriate antivirus software on all computers; and

   B. Respond to all virus attacks, destroy any virus detected, and document each incident.

3. Employee Responsibilities. These directives apply to all employees:

   A. Employees shall not knowingly introduce a computer virus into corporation computers;

   B. Employees shall not load diskettes of unknown origin; and

   C. Any employee who suspects that his/her workstation has been infected by a virus shall copy any pertinent screen message, IMMEDIATELY POWER OFF the workstation and call the Help Desk (ext. 4357).

4. Access Codes and Passwords: The confidentiality and integrity of data stored on corporation computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those areas and capabilities that are appropriate to each employee's job duties.

   A. Technology Department Responsibilities: The Network Administrator shall be responsible for the administration of access controls to all company computer systems. The Network Administrator, or designee, will process additions, deletions, and changes upon receipt of a written request from the end user's supervisor.
   Deletions may be processed by an oral request prior to receipt of the written request. The Network Administrator will maintain a list of administrative access codes and passwords, and keep this list in a secure area.

B. Employee Responsibilities. Each employee:

i. Shall be responsible for all computer transactions that are made with his/her User ID and password.

ii. Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords shall not be recorded where they may be easily obtained.

iii. Will change passwords at least every 90 days.

iv. Shall use passwords that will not be easily guessed by others.

v. Shall log out when leaving a workstation for an extended period.

C. Supervisor's Responsibility: Principals, managers and supervisors should notify the Network Administrator promptly whenever an employee leaves the corporation or transfers to another building/department so that his/her access can be revoked or modified. Involuntary terminations must be reported concurrent with the termination.

D. Human Resources Responsibility: The Human Resources Department will notify the Network Administrator bi-monthly of employee transfers and terminations. Involuntary terminations must be reported concurrent with the termination.

E. Physical Security: It is corporation policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

i. Employee Responsibilities: The directives below apply to all employees:

(a). Removable media (such as diskettes, CD's, etc.) are to be

stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.

(b). Removable media are to be kept away from environmental hazards, such as heat, direct sunlight, and magnetic fields.

(c). Critical computer equipment, e.g. file servers, must be protected by an uninterruptible power supply (UPS). A surge suppressor is to protect other computer equipment.

(d). Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold are to be avoided.

(e). Since the Director of Technology is responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities. This does not apply to temporary moves of portable computers for which an initial connection has been set up by the Technology Department.

(f). Employees shall not take shared portable equipment, such as laptop computers, out of the building without the informed consent of their supervisor. Informed consent means that the supervisor knows what equipment is leaving, what data is on it, and for what purpose it will be used. Employees are to exercise care to safeguard the valuable electronic equipment

assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.

(g). As a standard practice, employees shall shut down computer systems at the end of the day. This will guarantee all data files will be closed during backup procedures and any possible systems updates.

(h). Employees shall sign a copy of the Acknowledgment of Acceptable Use Policy, as acknowledgment of receipt and compliance with East Allen County Schools' Acceptable Use Policy.