

TECHNOLOGY AND PRIVACY IN THE WORKPLACE

Purpose: The purpose of this policy is to assert Gallatin County Board of Education's control over technology devices and the limitation of employee's privacy rights in the use of such technology.

Scope: This policy applies to all employees.

It is the policy of the Gallatin County Board of Education to provide for employees technology systems that improve their efficiency and overall effectiveness in carrying out their work assignments. Employees who accept and use technology systems provided by Gallatin County Schools cannot assume the information stored on such systems is private. Due to the need for periodic maintenance and emergency repair of technology equipment and programs, Administration must have unlimited access to employee's electronic files stored on the office electronic networks. Likewise, in the maintenance of voice and email messages, and Internet access, Administration may need to access to those files as may be necessary to ensure the proper operation of those systems.

It is not the intent to intentionally inspect the contents of employee's computer files, email, or voice mail or use of the Internet, in the normal day to day operation of office electronic equipment. However, employees must be aware that management's obligation to maintain equipment and software programs overrides the privacy of individuals who use the equipment.

Non-Administrative employees are prohibited from inspecting the computer files, voice mail, and email messages of other employees without their expressed consent.

Technology systems covered by this policy include the telephone voice mail, computer networks, Internet access and electronic mail. Employees are responsible to use these devices for business purposes only. The intentional misuse or abuse of technology provided by Gallatin County Schools may result in disciplinary action.

If the Superintendent determines that any employee has violated this policy, the offending employee will be subject to immediate discipline up to and including termination of employment.

POLICY: E-40

ACCEPTABLE USE OF ELECTRONIC INFORMATION RESOURCES & TECHNOLOGY

BACKGROUND

The Gallatin County Board of Education has invested in electronic information resources and technology in order to increase the productivity of employees.

This policy is based on the assumption that the majority of employees want to use information technology appropriately, but may be unaware of the laws, and regulations, and expectations guiding use. The adoption of an acceptable use policy involves educating all employees and providing legal and disciplinary boundaries for those whom may contemplate misuse.

PURPOSE AND INTENT

The Gallatin county Board of Education has adopted an Acceptable Use Policy(AUP) to guide access to information in electronic media, to information technology, and to networks. The purposes of this policy are: (1) to educate; (2) to provide protection against violations of privacy and misuse of resources, inappropriate or destructive behaviors which occur as a result of employee access to electronic information resources; and (3) to ensure that the technology resources are dedicated to improving service and raising productivity.

Each employee of Gallatin County Schools shall sign an Acceptable Use Policy Statement acknowledging their awareness of the policy and their understanding of individual responsibility related to policy compliance.

SCOPE

This policy includes a description of technical resources available to employees, related laws and policies, issues for additional consideration, and recommendations for maximizing the use of hardware, software, and information. The Policy extends to: computer hardware and peripherals; software; network services such as electronic mail and Internet; network access; storage devices; databases, files, and other repositories of information in electronic form. This policy applies to both on site and remote access.

APPLICABILITY

This policy applies to all employees.

RESPONSIBILITY FOR COMPLIANCE

Members of the Gallatin County Administrative Team (Superintendent, Assistant Superintendent, Technology Coordinator, Technology Technician, Principals, Program Coordinators, Guidance Counselors, School Psychologist, Director of Pupil Personnel, Special Education Director, and Head Teachers) are responsible for assuring that employees within their organizational authority have been made aware of the provisions of this policy, that compliance is expected and that intentional inappropriate use may result in disciplinary action.

Each individual is responsible for his/her own actions and the actions of those he/she knowingly permits to use assigned resources and passwords.

Identifying Appropriate and Inappropriate Use

Decisions about appropriate and inappropriate use of information technologies can be based on the same criteria, which guide decisions about use of other public agency assets. For instance:

- Public resources may not be used for private business or personal gain;
- Copyrights must be respected and authorship must be appropriately acknowledged;
- Vandalism, theft, prying, and willful destruction will not be tolerated; and,
- Passwords, personal access numbers, and security codes must not be exchanged or disclosed.

It is usually helpful to ask oneself these questions if you are not sure whether the way you are using technology violates the Appropriate Use Policy:

- Am I violating any other laws, regulations or policies? Have I protected individual privacy rights?
- Is this directly in support of my job duties and responsibilities?
- Does the way I am using technology adversely affect the productivity of others without good cause?
- If someone observed me doing this, either a colleague or member of the public, would I be uncomfortable: Would it give the impression that I was not doing my job or that this organization was misusing public funds:
- If I were saying it in email, would I say it in person?

MISUSE OF INFORMATION TECHNOLOGY AND THE LAW

Kentucky statutes identify criminal penalties for:

Criminal damage to Property Law Class D Felony KRS 512.020; A person is guilty of criminal mischief when, having no right to do so or any reasonable ground to believe that they have such a right, they intentionally or unintentionally deface, destroy, or damage any public agency data or technology property (data, computer programs, computer systems, computer networks, computers, etc.).

Unlawful Access To A Computer, Class C Felony Kentucky Criminal Statute DRS 434.840-434.860: A felony may be committed when an individual goes beyond assigned duties to: Knowingly and willingly, directly or indirectly, access, cause to be accessed, or attempt to access a computer system, data stored in a computer, or network purpose of altering, damaging, or destroying data or technology.

In simpler terms, these laws prohibit:

- Probing, which means using technology deliberately to gain access for which one is not authorized or to evade security procedures?
- Vandalism, which means altering or destroying data inappropriately, damaging hardware, software, or network components. Vandalism also includes deliberate attempts to restrict or degrade the access of others to data technology.

These laws do not prohibit systems administrators or others from examining files, transaction logs, or other information about an individual's use of technology if that examination is within the scope of their assigned responsibilities. If an employee with such responsibilities misuses their authority or the information to which they have access, they are also subject to discipline or penalty.

If an employee is absent from work or unavailable, the employee's supervisor may be provided with access to employee's workstation, files, and email account without the employee's prior notice or permission.

Open Records Laws, KRS 61.870 through 61.884 and KRS 171.410 through 171.720: The Kentucky Revised Statutes specifically include information in electronic form, computer programs, and systems software within the definition of "public record." This means that records held in computers may be inspected and copied in the same manner that paper records may be. Similarly, if a paper record is not subject to inspection under the provisions of these laws, then the record will not be subject to inspection if it is in electronic form. Electronic records are also subject to the provisions of the law related to records scheduling, retention, and disposal.

Employees must be aware that electronic mail logs, the content of electronic mail, Internet access logs, and the content of Internet sessions may be subject to inspection under the open records laws and are not necessarily private. The law is not clear on this issue at either the state or federal levels. Employees should remember that electronic mail, Internet access, and other resources are provided for carrying out assigned work.

There are numerous federal laws and regulations governing access to information managed by the Kentucky Department of Education, and the local school districts. The Appropriate Use Policy also assumes knowledge of and adherence to federal requirements. Information about managing the security of students records in electronic form may be found in “Program Review 95-KETS-152, Security of Student Records in the Kentucky Education Technology System.”

Pornography, Sexual Harassment, and Other Objectionable Materials: The introduction of Internet access and the ease with which electronic images and files may be transported increases the risk that pornography and other objectionable materials will be copied, created, or distributed through the use of public agency information resources. Pornography viewed by others inadvertently may constitute grounds for sexual harassment. Objectionable materials would include information from hate groups, information posted to harass or threaten, etc.

It is a violation of the Acceptable Use Policy to send, receive, store, create, display, or transmit pornography and other objectionable materials using Gallatin County School resources. This includes, but is not limited to:

- Placing such materials on or retrieving them from a public agency fileserver, hard drive, or other storage media;
- Sending or receiving pornography and objectionable materials through the network;
- Using public agency resources and/or network access to download from or post such materials to personally owned devices.

Copyright: Most software and much of the information posted on the Internet are copyrighted. Before software can be loaded on a computer or fileserver, Gallatin County Schools must have the legal right to install that particular version of the software. The software license will specify whether the rights purchased are for a single user on a single workstation, for multiple users, or for multiple workstations. Software may not be copied or shared outside the provisions of the agreement with the software publisher. Violations of software licensing agreements may constitute serious infractions of federal law and the violator may be subject to civil and/or criminal penalties.

Do not:

- Copy software without authorization from the publisher or copyright holder;
- Use software for which you do not have proof of legal right;
- Copy information or programs from the Internet and re-use or distribute it without acknowledging authorship and source;
- Assume that you can load the older version of software on another workstation when you install a software upgrade; and
- Take over a workstation without ensuring that the software already loaded is legal. When you assume responsibility for the workstation, you assume responsibility for the software.

Distributors of software and the Software Publishers Association have the right to audit Gallatin County Schools at anytime to ensure compliance with licensing agreements. For software loaded on file servers, the network administrator for that server has the responsibility for ensuring compliance with copyright laws. For application software loaded on an individual computer, the individual and the Technical Point of contact (TPOC) are responsible for ensuring that all resident software has been legally acquired. The user or TPOC must be prepared to show a software license certificate or copy of the purchase order for each piece of software loaded on that system.

Users must not load software on computers without notifying the TPOC. If the responsible party cannot show proof of license or proper authorization for a software program, the Gallatin County Schools has the obligation to remove the software from the computer or file server.

TECHNOLOGY AND GOOD PRACTICE

Avoid the “Futz” Factor: Industry studies estimate that the “Futz” Factor (as in “futz around”) consumes an average of five (5) hours per week for each computer user. The Futz Factor is the amount of time users spend in non-productive, non-work, related use of PCs and networks such as playing games, working on personal correspondence, chatting on email or the Internet, changing screen savers, and roaming the Web. As well as adversely impacting individual and organizational productivity, such use overloads the network and takes resources from legitimate activities.

GAMES: Games are not to be installed or played on Gallatin County School computers. The Internet is not to be used for the playing of games or participation in contests. Games are very resource intensive: remote access to games uses huge amounts of bandwidth and storing games on hard drives takes up space as well as memory..

(Instructional games and game-like software being evaluated or reviewed by staff in the course of their jobs are excluded from this prohibition.)

Personal Gain: Use of technology for the following is strictly prohibited:

- Private business;
- A non-work related club or organization;
- To obtain money, property or services for personal or private sector use; and,
- Political or religious purposes.

Netiquette. As mentioned before, a single individual using technology inappropriately can dramatically affect response time on the network. Having access to the network means having access to a shared highway or pipeline for sending and receiving information. This highway has limited capacity and can support only a certain amount of traffic at one time. Users should consider the impact of the work they are doing on the entire network, even when the work is will within the scope of the job. When possible, save resource intensive work for off-peak hours. Remember that images are particularly resource-intensive: One complex image may have resource requirements equivalent to that of 25,000 electronic mail messages.

Electronic Mail Is Immediate and Irretrievable! When email leaves your mailbox, it cannot be retrieved and its contents cannot be guaranteed to be confidential. Use good judgment and professional communications techniques when you use email. A time when you are extremely angry and frustrated is not a time to send email. If you would not make a statement to someone directly or would not put the content of your email in a memorandum, you should not send the same message via email. Also, remember that email can be forwarded to thousands of people within seconds without your approval, either intentionally or unintentionally.

Security: Security is every user's responsibility. If a user identifies a security problem within the network, that user is obligated to report the suspected problem to a systems administrator. Do not demonstrate the problem to other users.

Guidelines

- The user is responsible for the security of his/her user account. If passwords are distributed to others, the user is responsible for the actions of those to whom access is given. If the user leaves the workstation unattended with application open, the user is responsible for inappropriate use or security violations, which result. Choose and protect you passwords carefully. A good way to help secure your workstation temporarily is to set a screensaver password.
- Complete a virus scan before loading information you obtain by diskette.

- The use of “power on” passwords is not to be incorporated into the startup feature for any personal computer. Discuss storage of highly confidential information with the network administrator.
- Downloading programs from bulletin board services and installing personal shrink-wrapped software into Gallatin County School’s computers and/or networking environment is strictly prohibited without written approval from the network administrator. Bringing in such software increase the risk of viruses.

Security and Privacy

Users should be aware that the network administrator, to ensure appropriate content and use, might scan public folders(e.g. the x drive) on commonly shared file servers. If inappropriate or objectionable material is posted in these folders, the source of the material will be identified.

Non-public mail folders and data files are not routinely scanned without permission or cause. If a Program Director has cause to warrant inspection of access-restricted folders and files, the inspection will be documented after being approved by the Head Building Administrator.

GOOD PRACTICES

UNACCEPTABLE PRACTICES

<p>Be polite. Email and voice mail communications should be professional in content although they may be very informal in tone</p> <p>Protect your own privacy and respect the privacy of others. Remember that</p>	<p>Do not send abusive or offensive messages.</p>
<p>electronic communications can be forwarded to others without your consent. Do not assume that an email or voice mail is confidential.</p>	<p>Do not send electronic communications that contain ethnic slurs, racial epithets or anything that could be construed as harassment or abuse of others based on race, national origin, sex, sexual orientation, age, disability or religious or political beliefs. The same laws and regulations that apply to written communication may apply to electronic communications. Think carefully before you reveal your personal address, telephone number, or other sensitive information. Do not reveal personal information of another without their permission.</p>
<p>Send time critical and high-priority e-mails with a "Delivery Receipt" and/or "Read Receipt."</p> <p>Send "mass-mailings" of electronic attachments during low network usage times.</p>	<p>Do not call routinely to see if the recipient received your email. Use the return receipt feature. Call only when the receipt is not returned or when the recipient has not opened the mail.</p> <p>Do not send mass-mailings or graphics-intensive files at the same time to several recipients between 8:00a.m. and 4p.m. unless it is necessary</p>
<p>Use distribution lists only when necessary and with consideration for the recipients.</p>	<p>Do not use "All Users" and other large distribution lists simply for convenience. Doing so wastes people's time as well as network resources.</p>
<p>Use electronic bulletin board for those items that would be posted on a public</p> <p>Do not use email and voice mail to post</p>	<p>Non-Administrative employees are prohibited from inspecting the computer files, voice mail and email</p>
<p>private or non-work related communications such as advertisements,</p> <p style="text-align: center;">ACCEPTABLE USE AGREEMENT</p>	<p>messages of other employees without their expressed consent.</p>

**GALLATIN COUNTY SCHOOLS
EMPLOYEE
ACCEPTABLE USE AGREEMENT
FOR USE OF ELECTRONIC
INFORMATION RESOURCES
AND TECHNOLOGY**

I,

_____ have read the Gallatin
County School Employee Electronic
Information Resources and Technology.

By my signature, I am agreeing to
comply with this policy.

Date

Signature

Title