Acceptable Use Policy for Lawrence County Schools

INTRODUCTION

To ensure that students receive a quality education and that employees are able to work in a professional and intellectually stimulating environment, it is the policy of Lawrence County Schools to provide all students and employees with access to a variety of technology resources. All students and staff must acknowledge and adhere to this policy.

The creation of a large and varied technology environment demands that technology usage be conducted in legal and ethically appropriate ways, consistent with the Mission Statements and instructional goals of school systems. We recognize that the use of technology always requires attempts to balance the benefits against the possibilities of danger, security problems, and abuse. Rapid changes in technology and growth in the range of content available make this a constant challenge.

It is the intention of Lawrence County Schools that all technology resources will be used in accordance with any and all school system policies and procedures, as well as local, state, and federal laws and guidelines governing the usage of technology and its component parts. Additionally, it is implied that all students and employees will use the provided technology resources so as not to waste them, abuse them, interfere with, or cause harm to other individuals, institutions, or companies.

- The administrators of each school will be responsible for establishing specific practices to enforce this policy at individual schools.
- Highlights of this policy will be prominently displayed in all computer labs and posted on the district technology webpages of school systems.
- All technology resources, regardless of purchase date, location, or fund, are subject to this policy.
- Some of these policies pertain to technology equipment personally owned by school employees and students and brought into school facilities. All personal technologies used on any campus are subject to this policy and may be used only if such usage is in compliance with all school system policies, procedures, and guidelines as well as local, state, and federal laws.
- All electronic content stored on any external storage medium or personal off-site storage location that is brought to or accessed from a school campus is subject to all school system policies and guidelines as well as local, state, and federal laws.
- Any questions about this policy, its interpretation, or specific circumstances shall be directed to the District Technology Coordinator before proceeding.
- Students, Faculty, Staff, Student Teachers, volunteers, and any other individuals accessing technology resources are subject to the guidelines set forth in this acceptable use policy.

- Violations of this policy will be handled in a manner consistent with comparable situations requiring disciplinary and/or legal action.

POLICY STATEMENT

The primary goal of the technology environment is to support the educational and instructional endeavors of students and employees. Use of any and all technology resources is a privilege and not a right.

I. ACCESS

A. The use of all technology resources is a privilege, not a right. Inappropriate or suspected inappropriate use may result in a cancellation of those privileges pending investigation. Users must be aware that the school systems cannot assume any liability arising out of the illegal or inappropriate use of technology resources.

B. Users should not have any expectation that their usage of such resources is private. Reasonable efforts will be taken to maintain the security of technology resources, but the school systems cannot ensure that such security will not be penetrated or breached and cannot assume any liability arising out of any such penetration or breach of security.

C. Users should not purchase or dispose of software, hardware, peripherals, or other technology-related devices without consulting the District Technology Staff.

D. Individuals may use only accounts, files, software, and/or other technology resources that are assigned to, provided to, or approved for him/her.

E. Individuals may not attempt to log in to the network using any network account and/or password other than the login(s) assigned to him/her or allow someone to use his/her network account and/or password to access the network, email, or the Internet.

F. Individuals must take all reasonable precautions to prevent unauthorized access to accounts and data; and any other unauthorized usage within and outside the school systems. Any such unauthorized usage shall be reported immediately to the Local School Principal and/or the District Technology Director.

G. Individuals identified as a security risk may be denied access.

H. Any use of technology resources that reduces the efficiency of use for others will be considered a violation of this policy.

I. Individuals must not attempt to disrupt any computer services or data by engaging in activities including, but not limited to: spreading viruses, spamming, excess network and/or Internet activity, or modification of equipment or infrastructure.

J. Individuals must not attempt to modify technology resources, utilities, and configurations, change the restrictions associated with his/her accounts, or attempt to breach any technology resources, security system, or filtering system, either with or without malicious intent.

K. Personal technology-related devices such as laptops, PDAs, smartphones, iPods, etc., used on school grounds are subject to all items covered in this policy and should not access local area network or wide area network resources without the explicit permission of the District Technology Staff.

L. The District Technology Coordinator, and school system administrators will determine when inappropriate use has occurred and they have the right to deny, revoke, or suspend specific user accounts pending an investigation.

II. PRIVACY

A. To maintain network integrity and to ensure that the network is being used responsibly, District Technology Staff reserve the right to inspect any and all data, including data stored by individual users on individual school or personal devices. Users should be aware that activities may be monitored at any time, without notice.

B. Users should not have any expectation that their use of technology resources, including files stored by them on the school systems' network, will be private and will be secure from access by others. Reasonable steps will be taken to maintain the security of technology resources, but no assurance can be given that penetration of such security will not occur.

C. Because communications on the Internet are often public, all users should be careful to maintain appropriate and responsible communications.

D. The school systems cannot guarantee the privacy, security, or confidentiality of any information sent or received, either via the Internet, an email facility, telephone, or otherwise.

E. Users are encouraged to avoid storing personal and/or private information on the district and/or school technology resources.

F. The District Technology Staff performs routine backups in an effort to ensure continuity of business. There can be no assurance, however, that technology resources will be available within a particular time frame following an outage. In particular, that information that existed prior to an outage or malfunction, or that existed prior to a deliberate or inadvertent deletion, can be recovered. Users are responsible, without limitation, for the maintenance and backup of critical files and/or data.

G. Reasonable steps and procedures will be taken to secure student records, media center collections, and accounting information. Such information shall be backed up in a routine manner, with some information being maintained in secure offsite storage.

III. COPYRIGHT

A. Illegal copies of software may not be created or used on school equipment.

B. Any questions about copyright provisions should be directed to the District Technology Coordinator or the Local School Media Specialist.

C. Aspects involving the legal and ethical practices of appropriate use of technology resources will be taught to all students and employees in the system (i.e., as part of the Technology Education Curriculum, during lab orientation, network orientation, faculty meetings, etc.). There can be no assurance as to the extent and effectiveness of such training. Again, all questions regarding legal and ethical practices of appropriate use should be directed to the District Technology Coordinator.

D. Copyright is implied for all information (text, data, and graphics) published on the Internet. Web page authors will be held responsible for the contents of their pages. Do not "borrow" icons, sounds, or graphics from other pages without documented permission. It is the user's responsibility to secure proper usage permission.

E. Duplication of any copyrighted software is prohibited unless specifically allowed for in the license agreement and then, should occur only under the supervision and direction of the District Technology Staff.

F. All original copies of software programs, including those purchased with departmental funds, will be stored in a secure place.

G. For security and insurance purposes, the Local School Technology Assistants, and the district-level technology staff will be the only people with access to original software disks at a given school location with the exception of CDs required when accessing the program. System-wide software originals will be housed in a secure location.

H. In almost every case, a single copy of a given software package is purchased; it may only be used on one computer at a time. Multiple loading or "loading the contents of one disk onto multiple computers" (1987 Statement on Software Copyright) is NOT allowed.

I. Only the District Technology Coordinator or the Superintendent is authorized to sign license agreements for a school within the system.

J. The District Technology Staff is responsible for the installation of all software in use on the wide area network, local area network, and/or individual workstations/laptops within the school systems.

IV. EMAIL

A. Lawrence County Schools provide access to email for designated employees. They may also choose to offer student email accounts to a select portion of their student bodies. Student email accounts shall fall under the same guidelines as employee email accounts.

B. Technical support is provided for school email accounts used to conduct educational and/or instructional business.

C. Personal use of school email is discouraged and only permitted as long as it does not violate school policies and/or adversely affect others or the speed of the network.

D. When employing email, all users are responsible for maintaining professionalism at all times. Email communication sometimes lends itself to impulsive and informal communication. Users must be constantly mindful of the need to carefully review and reconsider email communications before responding to and/or sending emails. As a general rule, the content of an email should be acceptable to a general audience.

E. School email accounts may not be used for political activity, personal gain, commercial purposes, or profit.

F. School email accounts may not be used for attempting to send or sending anonymous messages.

G. School email accounts may not be used for sending mass emails unless for educational purposes or to parent lists.

H. School email accounts may not be used for posting or forwarding other users' personal communication without the author's consent.

I. Because email is not necessarily securely transmitted, employees must use discretion when sending, or encouraging the receipt of email containing sensitive information about students, families, school system employees, or any individuals. There can be no assurance that email will be confidential and/or private.

J. Lawrence County Schools make a reasonable effort to maintain (backup) email for normal business operations.

K. Incoming and outgoing email is filtered by the District for inappropriate content. However, no filtering system is foolproof, and material deemed inappropriate by individual users may be transmitted despite filtering.

V. INTERNET USE

A. The intent of Lawrence County Schools is to provide access to resources available via the Internet with the understanding that staff and students will access and use information that is appropriate for their various curricula.

B. All school rules and guidelines for appropriate technology usage as well as local, state, and federal laws apply to the usage of the Internet.

C. Teachers should screen all Internet resources before projecting them in the classroom.

D. Students gain access to the Internet by agreeing to conduct themselves in a considerate and responsible manner and by providing written permission from their parents.

E. Students are allowed to conduct independent research on the Internet upon receipt of appropriate permission forms.

F. Permission is not transferable and therefore may not be shared. Existing permission forms are valid until new forms are received. Students are required to have new forms signed when changing schools.

G. Students who are allowed independent access to the Internet have the capability of accessing material that has not been screened.

H. Internet activity can and will be monitored, along with other aspects of technology usage.

I. Internet access for all users is filtered through one central point by URL (web address) and by IP address and may be filtered by keyword.

J. URLs (web addresses) and IP addresses may be added to or deleted from the filtered list by the District Technology Staff.

K. Staff members may request to review filtered categories. Users requesting sites for blocking or unblocking must list specific URLs.

L. Successful or unsuccessful attempts to bypass the Internet filter by using proxies or other resources are a violation of this policy.

VI. WEB PUBLISHING

A. The Lawrence County Schools' websites are limited to usage associated with activities of the respective schools. The websites cannot be used for profit or commercial purposes.

B. The District Technology Staff reserves the right to reject all or part of a proposed and/or posted web page.

C. Each school webpage should contain contact information for the person responsible for the content.

D. All posted work must be of publishable quality with regard to spelling, usage, and mechanics.

E. All web page authors are responsible for the maintenance of their own pages.

F. All links should be checked regularly to ensure they are current and working. Pages that are not updated in a timely fashion, contain inaccurate or inappropriate information, violate copyright laws, or contain non-functional links will be removed, and the author will be notified.

G. Unfinished pages should not be posted until they are fully functional.

H. A teacher's primary web page should be accessible through the local school website. These pages should adhere to all school policies as well as local, state, and federal laws.

I. Links from pages housed on the school systems' websites to personal blogs, social networking sites, advertisements unrelated to school system business, and/or personal web pages are prohibited.

J. Pictures and other personally identifiable information should only be used with permission in writing from the parent/guardian of the student involved. No full names should be listed, only first names. No written permission is required for in-school broadcasts (i.e., morning news, announcements, class profiles, etc.).

K. Student posting of personal information of any kind on the school system's website or linking to personal information from the school system's website is prohibited. Personal information includes home and/or school address, work address, home and/or school phone numbers, full name, social security number, etc.

L. No written permission is required to list faculty/staff and their school contact information (phone extension, email address, etc.).

M. Infringement of copyright laws, obscene, harassing, or threatening materials on websites are against the law and are subject to prosecution.

VII. PARENTAL PERMISSIONS

It is the responsibility of the staff posting information on the web, requesting videos, or designing publicity or public relations information to obtain written parental permission.

VIII. CHILDREN'S INTERNET PROTECTION ACT (CIPA)

A. Lawrence County Schools comply with the Children's Internet Protection Act (CIPA) requirements, which includes:

- Implementing measures to block or filter Internet access to visual depictions that are obscene, child pornography, or harmful to minors.
- Monitoring the online activities of minors.
- Educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

IX. EXAMPLES OF INAPPROPRIATE USE OF RESOURCES

The following are examples of inappropriate activities when using any school network, email system, hardware, software, technology service, and/or Internet access:

A. Using another user's password or attempting to find out another user's password.

B. Sharing your own password.

C. Trespassing in another user's files, folders, home directory, or work.

D. Saving information on ANY network drive or directory other than your personal home directory OR a teacher-specified and approved location.

E. Downloading, installing, or copying software of any kind onto a workstation, your home directory, or any network drive.

F. Harassing, insulting, embarrassing, or attacking others via technology resources.

G. Damaging technology resources including but not limited to printers, telephones, computers, computer systems, or computer networks (this includes changing workstation configurations such as screen savers, backgrounds, printers, BIOS information, preset passwords, etc.).

H. Intentionally wasting limited resources such as Internet bandwidth, disk space, and printing capacity.

I. Accessing inappropriate material from off-site storage locations and/or removable storage devices.

J. Accessing inappropriate material from websites or attempting to bypass the Internet filter to access websites that have been blocked.

K. Sending, displaying, or downloading offensive messages or pictures.

L. Using obscene, racist, profane, discriminatory, threatening, or inflammatory language in a document, email, etc.

M. Using a digital camera, camera phone, or any other device capable of storing a still or video image to take inappropriate pictures or embarrassing without the subject's knowledge and/or consent. Editing/modifying digital pictures without the consent of the subject, especially with the intent to embarrass, harass, or bully.

N. Participating in online chat rooms without the permission/supervision of an adult staff member.

O. Posting any false or damaging information about other people, the school system, or other organizations.

P. Excluding information that is available to or being reported to the public, posting any personal information about another person without his/her written consent.

Q. Broadcasting network messages and/or participating in sending/perpetuating chain letters.

R. Violating copyright laws.

S. Plagiarism of materials that are found on the Internet.

T. Use of technology resources to create illegal materials (i.e., counterfeit money, fake identification, etc.).

U. Use of any school technology resource for personal gain, commercial, or political purposes.

V. Accessing any website or other resources by falsifying information.

This list is not all-inclusive but is intended to provide general guidance. Anything that would be considered inappropriate in "paper form" is also considered inappropriate in electronic form.

X. CONSEQUENCES OF VIOLATIONS

The consequences below relate to the use of technology hardware, software, and resources within Lawrence County Schools. Violations of the policy may result in additional disciplinary or legal action in accordance with the school system's code of conduct.

- Suspension of information network access.
- Revocation of information network access.
- Suspension of network privileges.
- Revocation of network privileges.
- Suspension of computer access.