

Carroll County Public Schools

Acceptable Use Policy

Overview

Purpose and Intent

Permissions & Agreements

Acceptable Uses

Users Defined

Software Installation

Right To Privacy

Misuse of Information Technology and the Law

Rights, Responsibilities, & Privileges

Network and Internet Regulations

E-Mail Regulations

Consequences

Internet User Agreement and Parent Permission Form

Overview

Telecommunications, electronic information sources and networked services significantly alter the way in which students gather information by giving them a much broader assortment of informational sources. In the past, instructional personnel, library media specialists and community members could pre-screen materials to assure that the material was both beneficial and non-offensive. Board Policy 08.1 requires that all such materials be consistent with the district-adopted guides, supporting and enhancing the current curriculum while taking into account the various instructional needs, learning styles and developmental levels of the students. Telecommunications, in particular, the Internet, may open classrooms to electronic information resources that have not been screened by educators for use by students of various ages.

The Board of Education recognizes that as information accessibility changes, those changes will also alter the way in which instruction is provided and learning takes place. The Board supports access by students to rich information resources along with the development by staff of appropriate skills to analyze and evaluate such resources. The Board also recognizes that access to information for informed decision making is a necessity in today's society as well as being a fundamental right in a free and democratic society.

Electronic information research skills are now a basic skill needed for preparation of citizens and future employees. The Board of Education expects the staff to provide access and practical usage of such information throughout the curriculum and requires the staff to provide guidance and instruction to students in the appropriate use of such resources.

Purpose and Intent

The Carroll County Public Schools have adopted an Acceptable Use Policy to guide access to electronic media, to information technology and to networks. The purposes of this policy are to: educate; provide protection against violations of privacy; provide acceptable rules of on-line behavior; provide guidelines for access privileges and penalties for policy/procedural violations.

Permissions and Agreements

All adults accessing the Carroll County Public Schools network, whether staff members or members of the community, shall sign an agreement form after reading the acceptable uses, rules of on-line behavior, access privileges and penalties for policy/procedural violations. The required form will be kept on file at the appropriate site and be viewed as a legal, binding document.

All students utilizing the Carroll County Public Schools network and are under the age of 18, are required to have a Internet User Agreement and Parent Permission Form signed, by both the student and their parent(s). The required form will be kept on file at the appropriate site and be viewed as a legal, binding document.

All students utilizing the Carroll County Public Schools network and are 18 and above, are required to have signed the student portion of the Internet User Agreement and Parent Permission Form. The required form will be kept on file at the appropriate site and be viewed as a legal, binding document.

Acceptable Uses

Access to all electronic resources on the Carroll County Public Schools network is a privilege and carries with it responsibilities. The following are general policies that apply to all users, student and adult.

- The Carroll County Public Schools maintain the right to limit access to software, hardware, Internet, and the local area network.
- The Carroll County Public Schools will not be responsible for damages caused by loss of data or other work that results from delays, non-deliveries, missdeliveries, or service interruptions for any reason.
- Security on any computer system is a high priority. If any user identifies a security problem, they must notify a network administrator immediately and not demonstrate the problems to others.
- Vandalism shall result in cancellation of privileges. Vandalism is defined as any attempt to harm or destroy data, hardware or software of the Carroll County Public Schools network or any other network connected to the Carroll County Public Schools network. This also applies to workstations not a part of the network. This includes, but is not limited to the following:

- The intentional uploading, downloading or creation of viruses.
 - Altering workstations in any way, such as installing unapproved software or changing hardware settings
 - Disrupting network performance
 - Disrupting other users on the network
 - Downloading and/or distribution of software, without permission.
 - Changing other users passwords
 - Logging on as other users
- All users must use their own ID and password. The only exception is for students at the Primary level (K – P3). Teachers and/or aides may log on for students at this level.
 - All users will use a pre-defined network location for storage of files. Files located on individual workstations are subject to erasure without warning by technical staff during upgrades, maintenance or re-installs.
 - All workstations will be shut down at night to decrease energy usage.
 - No workstation should ever be left on and logged into the network. If a staff member does leave their station logged on and an unauthorized user gains access to the network, then the staff member who's at fault will be held liable for any damages.
 - No student will have access to the Internet without direct adult supervision. This includes before and after school. Any student violating this will face consequences as defined in the Uniform Code of Student Conduct. The staff member who has responsibility for that student will be dealt with by the building principal and/or district administrative staff.
 - E-Mail shall be used for approved school related purposes only. Its' purpose is to provide effective communications between staff members and themselves as well as other professionals in education. The following is types of E-mail, though not limited to these, shall not be used for:
 - To conduct personal business or carry on personal relationships
 - To rebuke, embarrass, or strike-out at others
 - To harass or play practical jokes on others
 - To send chain letters and other non-work related correspondence
 - To solicit money or participation in political or religious activities
 - Once e-mail has been opened, it shall be moved to a personal folder and deleted from the In-Box. Leaving mail in the In-Box builds up mail on the Exchange Server and slows performance. If necessary, e-mail accounts will be limited to their size, cutting off user e-mail until they have performed these deletions.

Users Defined

All Carroll County staff will be given access to the network. In using the network they are expected to comply with all of the provisions of this policy and all district standards. E-mail accounts will be assigned for all staff members, though workstation licenses will be limited as determined by the District Technology Coordinator and/or School Technology Coordinator. Staff members include all full time employees. Long term

substitute teachers may be included upon request. When accounts are set up, a generic password will be given. It is the responsibility of the staff member to immediately change their password to prevent unauthorized access under their ID. It doesn't take hackers long to guess at passwords, therefore, all liability for such misuse lies with the staff member. All staff members will be required to have a signed form on file.

Students of Carroll County Public Schools have access to the network as a part of their school studies. Internet access and E-mail is limited to those students who bring in signed permission forms. It is the responsibility of the school staff to monitor student network access and Internet Usage. Any staff member not properly supervising may be reported to their building principal and/or the Board of Education.

Community members may be given access to the network upon request for limited access and for a limited time period. They will follow the same guidelines as established for Carroll County staff members. They will be required to have a signed form on file.

Software Installation

Students, unless directed by a staff member, shall under no circumstances install software to a workstation. Staff members who wish to install software should notify their School Technology Coordinator or District Technology personnel. Any unauthorized software that causes a network and/or workstation problem may result in that software being removed and/or administrative rights being taken away from the user. *The workstations available to students and staff of Carroll County are for work purposes only.* They are not entertainment centers, game centers, etc.

The following types of software are not allowed on workstations:

- Games
- Personal Business
- Personal Communications

Right To Privacy

All network administrators have the right to access information stored in any user directory, on the current users screen, or in e-mail. Users are advised not to place personal, confidential documents in their users network directory or on the local workstation. Network management and monitoring software may be used to randomly access student and staff network logs, Internet logs, individual user directories, etc.

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 KRS 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 a 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 and 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 the 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. Employees should remember that electronic mail, Internet access, and other resources are provided for the purpose of carrying out assigned school related work activities only.
- There are numerous federal laws and regulations governing access to information managed by the 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 student 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, sexually explicit matter 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, and transmit pornography, or sexually explicit matter and other objectionable materials using District 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, receiving pornography, or sexually explicit matter 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, the District 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 the District 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 District computers without notifying the TPOC. If the responsible party cannot show proof of license or proper authorization for a software program, the District has the obligation to remove the software from the computer or file server.

Rights, Responsibilities, and Privileges

This document of the Terms and Conditions for use of the Carroll County Public Schools network must be signed by all students and adults to get an individual user account. Its' purpose is to ensure a clear understanding of network access, Internet usage, and Electronic mail.

Network and Internet Regulations

Violation of any of the following terms and conditions for network access and Internet usage will result in immediate loss of network access and services, with the exception of required instructional sites as determined by each school, as well as possible future access.

The use of your account must be in support of education and research and consistent with the educational objectives of the Carroll County Public Schools.

- a. You may not give your password to anyone
- b. You may not use or alter anyone else's account
- c. You may not offer Internet access to any individual via your account
- d. You may not break into or attempt to break into the school network or any other network
- e. You may not create or share computer viruses
- f. You may not destroy another person's data
- g. You may not use MUD (Multi User games) on the network or via the Internet
- h. You may not monopolize the resources of the network by sending large amounts of e-mail, sending chain mail, using resources for games or running large programs or applications over the network during the day
- i. You are not permitted to get from or put onto the network any copyrighted material (including software), or threatening or obscene material. This also applies to workstations.
- j. No illegal activities are permitted on the network
- k. All communications and information accessible via the network should be assumed to be public property
- l. You may not use Internet mail services, such as HotMail.

Users should notify their School Technology Coordinator or District Technology personnel of any violations of this contract by other users or outside parties. This may be done anonymously.

E-Mail Regulations

1. Do not send unsolicited mail to others
2. Do not send chain letters
3. Save attachments and scan for viruses before opening any attachment.
4. Do not send EXE or BAT files through E-Mail
5. Do not reveal any personal information to unknown users
6. Do not leave e-mail up and active while you are away from your room or office

***Note: Electronic mail is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.

***Note: Log files will be reviewed periodically and randomly as to user access to the Internet and locations they have visited. This information will be turned over to building principals and Board of Education administrators.

Consequences

- Violations may result in loss of access for anyone violating the Acceptable Use Policy for Carroll County Schools. Loss may be short term to permanent.
- Additional disciplinary action may be determined at the building level in line with existing practices regarding inappropriate language or behavior for students.
- Additional disciplinary action may be determined at the building level and/or district level for any system violations and/or Acceptable Use violations by staff members, such as giving out passwords, trying to access closed areas, lack of supervision of students accessing the network and/or Internet, etc.

When applicable, law enforcement agencies will be notified and individual violators will face possible criminal charges, as well as possible expulsion for students and possible termination of employment for staff members.

XVII. Agreement and Parent Permission Form

In compliance with the Drug-Free Schools and Communities Act, 1989, Code 86.200, all parents and students are to be given a copy of the standard of conduct and the statement of disciplinary sanctions.

Please read the Uniform Code of Student Conduct manual with your child, check the statements below, sign and return this page to your child's school. Thank you. (Submission of this page is required for registration)

Carroll County Schools

Student's full name: (Please Print)

School: _____ Grade: _____ Homeroom: _____

____ As the parent or legal guardian of the student above, I have received a copy of the Carroll County Schools Uniform Code of Student Conduct manual and have read with my child the policies therein, including those regarding alcohol, tobacco, other drugs and weapons.

____ As parent or legal guardian of the student above, I grant permission for the Carroll County School District to enable a feature of web based individual learning Plan (ILP) software, which will permit my student to invite third parties to have access to his/her ILP information via the internet. (Refer to Individual Learning Plan Web Release, Section XXVI)

____ As the parent or legal guardian of the student above, I verify that my child and I have read the school district's Internet Code of Conduct and hereby agree that my child will comply with the polices for accessing information over the network in a responsible fashion while honoring all relevant laws and restrictions. We understand that we will be held liable for any violation of the rules.

____ I grant permission for my child to have his/her picture or student work appear and be identified on the Carroll County Public Schools web pages, video conferences, or included in print and broadcast media.

____ I grant permission for my child's contact information to be released to community organizations that provide charitable student services. Example: Shop with A Cop, and other giving programs.

Student's Signature: _____ Date: _____

Parent/Guardian Signature: _____ Date: _____

Home Phone: _____ Work Phone: _____