2012-13 CISD Student Technology Acceptable Use Policy

Information Technology Guidelines for Students

The Carroll Independent School District provides technology resources to its students and staff for educational and administrative purposes. The goal in providing these resources is to promote educational excellence in the District's schools by facilitating resource sharing, innovation and communication with the support and supervision of parents, teachers and support staff. The use of Carroll ISD technology resources is a privilege, not a right, and should be treated as such.

Carroll ISD firmly believes that the value of providing information, interaction, and research capabilities far outweighs the possibility that users may obtain material that is not consistent with the educational goals of the district. Carroll ISD complies with Federal regulations regarding internet filtering in order to limit user access to inappropriate content.

Proper behavior, as it relates to the use of computers, is no different than proper behavior in all other aspects of Carroll ISD activities. All users are expected to use the computers and computer networks in a responsible, ethical, and polite manner. Any user who does not comply with policies and procedures may face appropriate disciplinary actions, including all student discipline management techniques, and discontinued computer access.

The Superintendent or designee will oversee and/or monitor the District's electronic communications systems. **Users should not have any expectation of privacy when using District systems**.

Definition of District Technology Resources:

The District's computer systems and networks are any configuration of hardware and software. The systems and networks include all of the computers hardware, operating system software, application software, stored text, and data files. This includes but is not limited to electronic mail, local databases, externally accessed data (i.e. the internet), CD-ROM, optical media, clip art, digital images, digitized information, communications technologies, and new technologies as they become available. **The District will at its own discretion monitor any technology resource activity without further notice to the end user.**

Acceptable Use:

The District's technology resources will be used only for learning, teaching, and administrative purposes consistent with the District's mission and goals. The District email system should not be used for mass mailings except for official school business. Personal commercial use of the District's system is strictly prohibited.

Other Issues Applicable to Acceptable Use Are:

1. **Copyright**: All users are expected to follow existing copyright laws.
2. **Supervision and permission**: Student use of the computers and computer network is only allowed when supervised or granted permission by a Carroll ISD staff member.
3. **Network Access**: Attempting to log on or logging on to a computer or email system by using another's password is prohibited. Helping others to violate this rule by sharing information or passwords is unacceptable.
4. **Improper Use Is Prohibited**: This includes, but is not limited to the following:
   - Submitting, publishing or displaying any defamatory, cyber bullying, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages either public or private
   - Using the network for financial gain, political or commercial activity
   - Attempting to or harming equipment, materials or data
   - Attempting to or sending anonymous messages of any kind

- Using the network to access inappropriate material
- Knowingly placing a computer virus on a computer or the network
- System users should avoid actions that are likely to increase the risk of introducing viruses to the system, such as opening email messages from unknown senders and loading data from unprotected computers
- Accessing of information resources, files and documents of another user without authorization
- Attempting to or accessing technology resources without authorization
- Attempting to or bypassing school proxy servers to access the internet
- Posting personal information about others without proper authorization
- Attempting to "hack" into network resources
- Storing inappropriate information (i.e. programs and .exe files) in home directories or student shares

System Access:

Access to the District's network systems will be governed as follows:

1. Students will have access to the District's resources for class assignments and research with their teacher's permission and/or supervision. Students will be given a limited amount of space to store educational files on the network. Files should be kept on the districts file storage instead of on local computers since local computers are not backed up.
2. Password confidentiality is required, and password sharing is not permitted with students, staff, or others.
3. Any system user identified as a security risk or having violated District Acceptable Use Policy may be denied access to the District's system. Other consequences may also be assigned.

Individual User Responsibilities:

The following standards will apply to all users of the District's electronic communications systems and resources:

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by district guidelines.

Vandalism Prohibited:

Any malicious attempt to harm or destroy District equipment or materials, data of another user of the District's system, or any of the agencies or other networks to which the District has access is prohibited. Deliberate attempts to degrade or disrupt system performance will be viewed as violations of district guidelines and, possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses, and the use of system hacking programs and utilities. Any interference with the work of others, with or without malicious intent, will be construed as vandalism. Vandalism, as defined above, may result in the permanent cancellation of system use privileges, possible prosecution, and will require restitution for costs associated with system restoration, hardware, and software repair or replacement.

Forgery Prohibited:

Forgery or attempted forgery of electronic messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.

Some Technology Resources Prohibited:

System users are prohibited from connecting the following technology resources: hubs, switches, routers, wireless access points/devices. Additionally, system users are prohibited from installing or setting up any device

that would alter the network topology or any server-based software or technologies without approval from the Executive Director of Technology.

Information Content/Third Party Supplied Information:
System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communications systems outside the District's networks that may contain inaccurate and/or objectionable material. A student bringing prohibited materials into the District's electronic environment will be subject to a suspension and/or a revocation of privileges on the District's system and will be subject to disciplinary action in accordance with district policies which could result in loss of credit.

Network Etiquette:
System users are expected to observe the following network etiquette:

1. Use appropriate language: swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited
2. Pretending to be someone else when sending/receiving messages is prohibited
3. Submitting, publishing or displaying any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages, public or private, is prohibited
4. Using the network in such a way that would disrupt the use of the network by other users is prohibited
5. Students should never make appointments to meet people whom they meet online and should report to a teacher or administrator if they receive any requests for such a meeting

Participation in Social Networking and Other Web Sites, and Chat Rooms:
Students participating in social networking web sites or chat rooms using District electronic resources should assume that all content shared, including pictures, is public. Students should not respond to requests for personally identifying information or contact from unknown individuals.

Consequences of Improper Use:
Any attempt to violate the provisions of these guidelines may result in revocation of a user's account, regardless of the success or failure of the attempt. Improper or unethical use may result in disciplinary actions consistent with the existing Student Code of Conduct, and/or appropriate legal actions as prescribed by law.

Disclaimer:
The district's technology resources are provided on an "as is, as available" basis. The district does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein.

The district does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not the district.

The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district's Electronic Communications System.

Term:
This policy is binding for the duration of a student's enrollment in the Carroll Independent School District. This policy must be reviewed and signed **annually** at the start of each school term.