2017-18 CISD Volunteer Technology Acceptable Use Policy

Volunteer Agreement for use of Carroll ISD Technology Resources

Using CISD's technology resources you will be able to communicate with others around the world through the Internet and other electronic information systems/networks, and will have access to hundreds of databases, libraries, and computer services all over the world. With this educational opportunity also comes responsibility. It is important that you read the Volunteer Technology Acceptable Use Policy and the agreement form.

Inappropriate system use will result in the loss of the privilege to use this educational and administrative tool. Please note that the Internet is a network of many types of communication and information networks. It is possible that you may run across some materials that you find objectionable. While the District will use filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use as outlined in the Acceptable Use Policy.

VOLUNTEER AGREEMENT:

I, _____, understand that my computer use is not private and that the District will monitor my activity on the computer system. I have read the Acceptable Use Policy for Carroll ISD and agree to abide by its provisions. In consideration for the privilege of using the District's Technology Resources and in consideration for having access to the public networks, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, the system, including, without limitation, the type of damages identified in the District's policy and administrative regulations.

I realize that I am responsible for the monitoring of network use by students under my supervision. I will immediately report any violations of the Acceptable Use Policy to the campus principal, or the Executive Director of Technology.

Volunteer Name _____ Date _____
(Print Name)

Volunteer Signature _____ Campus / Location _____

2017-18 CISD Volunteer Technology Acceptable Use Policy

Information Technology Guidelines for Volunteers

The Carroll Independent School District provides technology resources 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. This document is intended to clarify those expectations as they apply to computer and network usage and is consistent with District Policy as well as guidelines at the local, state, national, and international levels. Any user who does not comply with policies and procedures may face appropriate disciplinary actions. The Superintendent or designee will oversee and/or monitor the District's Technology Resources. Users should not have any expectation of privacy when using any District system.

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 hardware, operating system software, application software, stored information, 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, 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 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.

Improper Use Includes:

1. 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;
2. Attempting to or harming equipment, materials or data;
3. Attempting to or sending anonymous messages of any kind;
4. Using District resources for personal commercial purposes;
5. Using the network to access inappropriate material;
6. Knowingly placing a computer virus on a computer or the network;
7. 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,
8. Accessing of information resources, files and documents of another user without authorization,
9. Attempting to or accessing technology resources without authorization;
10. Using proxy servers or bypassing security and gain access to the internet or network resources;
11. Posting personal information about others without proper authorization;
12. Attempting to "hack" into network resources;
13. Storing inappropriate information (i.e. programs and .exe files) in home directories;
14. Swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language is prohibited;
15. Using the network in such a way that would disrupt the use of the network by other users is prohibited;
16. Responding to requests for user credentials via email, this is called Phishing. Do not provide logins and passwords to websites unless you know they are district approved websites.
17. Attempts to degrade or disrupt resource performance;

18. Any interference with the work of others, with or without malicious intent;
19. Forgery or attempted forgery of electronic messages or data, or violation of copyright laws;
20. Pretending to be someone else when sending/receiving messages.

System Access:

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

1. Users with accounts will be required to maintain password confidentiality by not sharing the password with students or others. Your username and password should be protected from unauthorized use at all time. Do not post any of this information where others can view it and do not send it via email. Use passwords that are difficult to "hack" and make sure not to store passwords in easily accessed locations.
2. With the approval of the immediate supervisor, district employees will be granted access to the District's systems.
3. Any system user identified as a security risk or having violated District Acceptable Use Guidelines may be denied access to the District's system. Other consequences may also be assigned.
4. You should lock your workstation to secure your computer whenever it is not in use. If you are logged into the network, leaving a computer unlocked and unattended enables anyone to potentially access your gradebook, email, and/or other personal or information-sensitive files. Workstations can be locked by pressing "CTRL -ALT-DEL" and selecting the "Lock Workstation" option.
5. The individual in whose name a system account is issued will be responsible at all times for its proper use.
6. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by district guidelines.

Prohibited Network Changes:

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. Setting up a wireless access point, whether connected to the network or not, is prohibited.

Data Security:

As part of your duties, you may have access to confidential information such as student social security numbers. Caution must be taken to insure this data is not exposed to those without an educational need to know. A data file that contains confidential information could be at risk for inadvertent release, and can damage the financial, professional or emotional futures of others, thus this information must be handled appropriately.

1. Limit data exports to only the necessary information on the required people.
2. Do not leave data files in an unsecure location such as an unattended automobile.
3. Access to confidential information should be given on an as needed basis. If you are able to access confidential information that you do not need, you are required to report it to the manager of that data system.
4. Be very cautious in transporting data files. Data transported on flash drives or external drives can be lost easily.
5. Cloud based storage systems such as Google Drive and Dropbox are also susceptible to leaks especially if users do not correctly configure sharing permissions. Therefore public web-based file sharing tools should not be used to store confidential information.
6. Data files containing confidential information that are leaving the district via email or on media, must be encrypted.

Information Content/Third Party Supplied Information:

System users 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. An employee bringing prohibited material into the school's electronic environment will be subject to disciplinary action in accordance with district policies which could result in termination of employment.

Information Content/Third Party Supplied Information:

System users 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 Volunteer bringing prohibited material into the school's electronic environment will be subject to disciplinary action in accordance with

district policies.

Maintenance of Local Hard Drives:
You are personally responsible for making backups of any data files that are stored on your local hard drive. Files stored in user home directories on district servers will be backed up by the Technology Department.

Computer Hardware:
1. All hardware purchases must go through the District Technology Department.
2. All hardware must be purchased through and shipped to the technology department with documentation listing campus name and contact.
3. Absolutely no one except district technicians, certified/trained computer facilitators, or vendors approved by the Executive Director of Technology is authorized to install computer hardware on any district equipment.
4. Campus computer systems may not be modified, upgraded, or replaced with donated equipment without the prior approval of the technology department.
5. To maintain accurate physical inventory campus computer systems are not to be moved from one room to another room on the same campus or to another campus, without the prior approval of the campus technology facilitator.

Termination/Revocation of System User Account:
The district may suspend or revoke a system user's access to the district's system upon suspected violation of district policy and/or administrative regulations regarding acceptable use. Termination of a volunteer's account will be effective on the date the Executive Director of Technology, Principal, or designee receives notice of user withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

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 handbooks up to and appropriate legal actions as prescribed by law.

Disclaimer:
The district's system is 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 Technology Resources.

Term:
This policy is binding for the duration of your service with the Carroll Independent School District.