



## 2022-23 CISD Student Technology Acceptable Use Policy

### Agreement for Student use of Carroll ISD Technology Resources

Using CISD's technology resources students 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 and your child read the Student Technology Acceptable Use Policy, Board Policies CQ, FNCE, and agreement form and discuss requirements together. Inappropriate system use could result in the loss of privilege to use this educational tool. Please note that it is possible that your child may run across content that you may find objectionable. While CISD will use filtering technology to restrict access to such material, it is not possible to absolutely prevent such access.

#### **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. 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 hardware, software and data. This includes but is not limited to email, local databases, externally accessed data (i.e. the internet) network storage, 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. Personal commercial use of the District's system is prohibited. Student use of CISD computers and is only allowed when supervised or granted permission by a Carroll ISD staff member. All users are expected to follow existing copyright laws.

#### **Prohibited Improper Uses:**

This includes, but is not limited to the following:

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. Using the network for financial gain, political or commercial activity



## 2022-23 CISD Student Technology Acceptable Use Policy

3. Attempting to or harming equipment, materials or data
4. Attempting to or sending anonymous messages of any kind
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. Attempting to or bypassing school internet filters
11. Posting personal information about others without proper authorization
12. Attempting to “hack” into resources or use of hacking software
13. Storing inappropriate information (i.e. programs and .exe files) in home directories or student shares
14. Attempts to degrade or disrupt resource performance
15. Passwords are confidential. 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.
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. Any interference with the work of others, with or without malicious intent
18. Forgery or attempted forgery of electronic messages or data is prohibited
19. Pretending to be someone else when sending/receiving messages is prohibited
20. Systems may not be used for, or in support of, illegal activities, or for any other activity prohibited by district guidelines.
21. Installing any software on the device, including: programs, apps, extensions, and other software. All software must be preapproved and installed by district technicians.

### **Technology Instructional Resources Acceptance:**

In accordance with the Children’s Internet Protection Act, Carroll ISD educates staff and students regarding appropriate online behavior to ensure Internet safety, including use of email and Web 2.0 resources, and has deployed filtering technology and protection measures to restrict access to inappropriate content such as those that are illegal, are harmful, or contain potentially offensive information.

Beginning with the 2019-2020 school year, CISD is implementing a new process to review instructional software. Instructional software, including web based tools, and apps are being vetted by the Technology, Curriculum & Instruction, and Special Programs Departments to maximize student data security and to provide the best quality instructional tools. Instructional software is reviewed and scored based on data security, student privacy, online safety, quality of content, and accessibility.

For students under the age of 13, the Children's Online Privacy Protection Act (COPPA) requires additional parental permission for education software tools. Accepting the district’s AUP gives permission for CISD students to use the district’s approved software. The list of pre-approved software can be found at: <https://www.southlakecarroll.edu/Page/404> . This list will continue to change as more products are reviewed and approved. If parents wish to change their decision regarding acceptance or revocation of the district’s AUP made during annual verification before school begins, they may do so in writing to the appropriate campus administrator at any time during the school year.

### **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. Files



## 2022-23 CISD Student Technology Acceptable Use Policy

- should be kept on the districts file storage instead of on local computers since local computers are not backed up.
2. 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.
  3. The individual in whose name a system account is issued will be responsible at all times for its proper use.

### **Some Technology Resources Prohibited:**

Installing or connecting the following is prohibited: 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.

### **Online Communications:**

Students communicating online using social networking sites, or other websites 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. 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. Students must ensure that online postings made in or out of school will not impede your school's effectiveness or efficiency or otherwise disrupt the school environment. You must be careful not to engage in comments that could adversely affect your school (i.e., damage the school's reputation) or interfere with your ability to participate in school activities.

### **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 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.