



DICKSON COUNTY SCHOOLS

Technology Acceptable Use Agreement

Dickson County Schools (DCS) recognizes the value of computer and other electronic resources to improve student learning and enhance the administration and operation of its schools. DCS encourages the responsible use of computers; computer networks, including the internet; and other electronic resources in support of the mission and goals of the school system.

The DCS Acceptable Use Agreement shall govern all use of technology devices, digital resources, digital and online curriculum, student and staff data and personal information, and network infrastructure. Because technology is constantly changing, not all circumstances can be anticipated or addressed in this agreement. All users are expected to understand and comply with both the “letter” and the “spirit” of this agreement and show good judgment in their use of these resources. By using or by accessing district facilities or services, the user agrees to abide by this agreement.

Rights and Responsibilities

DCS is committed to complying with applicable information security requirements and relevant information security standards and protocols. These requirements include, but are not limited to the following:

The Family Educational Rights and Privacy Act ([FERPA](#))

Children's Internet Protection Act ([CIPA](#))

Individuals with Disabilities Education Act ([IDEA](#))

Children's Online Privacy Protection Act ([COPPA](#))

Health Insurance Portability and Accountability Act ([HIPAA](#))

Users of the DCS network, technology and sensitive digital data resources are required to adhere to state and federal law as well as board policy. Any attempt to break those laws or policies may result in discipline or litigation against the offender(s) by the proper authority. DCS will provide any information necessary in order to fully cooperate with the appropriate authorities in the civil and/or criminal process.

Privacy

Users should not assume that any files or communications created, transmitted, deleted or displayed using DCS technology resources or stored on DCS servers and devices will be private unless protected by local board, state or federal laws (such as medical records or student records under FERPA).

At any time, DCS may, (1) monitor, track, and/or log network access, communications, and use; (2) monitor and make changes to server storage space; and (3) access, review, copy, store, delete, or disclose the content of all user files, regardless of storage medium, for any lawful purpose. Such purposes may include, but are not limited to, maintaining system integrity, security, or functionality, ensuring compliance with board policy and applicable laws and regulations, protecting the school system from liability, and complying with public records requests.

Acceptable Use Details

DCS provides students and staff with computing and internet access to further educational goals and objectives. Access is a privilege, not a right, and therefore, entails responsibility. The district provides computers and a computer network for students and staff who agree to act in a considerate and responsible manner. The network is available to conduct research, save student work and files, and communicate with others via electronic media. Teachers, administrators, and other school personnel should ensure district data systems are used in a responsible, efficient, ethical, and legal manner, and such use must be in support of the district's business and education objectives.

Security

Security of student and staff data is a priority of the DCS school system. There are technological requirements in place to help protect student work, student communication access, and Personally Identifiable Information (PII) data for everyone. All employees and students are expected to follow all security-related guidelines listed below.

1. Users are prohibited from accessing any DCS technology, online instructional content or any other DCS resource using another individual's username or password for any reason. Violations could result in loss of privileges or possible legal consequences.
2. Users should never share their password with anyone. Employees and students are responsible for ensuring that their passwords and login information is kept confidential.
3. Users must respect the privacy of others. When using e-mail, chat rooms, blogs, or other forms of electronic communication, students and employees must not reveal personal identifying information or information that is private or confidential, such as the home address or telephone number, credit or checking account information, or social security number of themselves or fellow students. Violation may result in legal or criminal action.
4. If a user identifies a security problem on a technological resource, he or she must immediately notify a system administrator. Users must not demonstrate the problem to other users. Any user identified as a security risk will be denied access.
5. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).
6. Users must respect the privacy of others. When using e-mail, chat rooms, blogs, or other forms of electronic communication, students must not reveal personal identifying information or information that is private or confidential, such as home address or telephone number, credit or checking account information, or social security number of themselves or fellow students.
7. Users are prohibited from engaging in unauthorized or unlawful activities, such as "hacking" or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems, or accounts.
8. The use of anonymous proxies to circumvent content filtering is prohibited.
9. Students and staff are prohibited from recording other students and staff, whether voice or video, without parent permission or as instructed by the teacher for educational purposes. At no time shall students or staff operate any device with video, voice recording or picture taking capabilities in a locker room, classroom, bathroom, or other location where such operation may violate the privacy right of another person. Such recordings shall also not be posted, shared or made available to other users without the express written consent from parents and guardians. All instructional recordings must comply with local, state and federal privacy and safety regulations.

Educational Purpose

School system technological resources are provided for the purpose of instruction, accessing information, conducting research, lesson preparation, communication, and/or other information gathering and sharing as it relates to education. Every year, students are educated on appropriate online behavior, including interacting with other individuals on social networking websites and cyber-bullying awareness and response. All DCS users are subject to the following guidelines.

1. School system technological resources are provided for school-related purposes only. Acceptable uses of such technological resources are limited to responsible, efficient, and legal activities that support learning and teaching. Use of school system technological resources for commercial gain or profit is prohibited.
2. Users may not use the DCS network for personal or commercial gain or for personal political purposes.
3. Violations of acceptable uses of district technology and digital resources may result in one or more of the following consequences: loss or suspension of use or access privileges; disciplinary action as outlined under applicable district policies and procedures; or civil or criminal liability under applicable laws.
4. During the instructional day, all instructional staff are to make reasonable efforts to supervise student use of the district's internet system in a manner that is appropriate to the student's age and circumstances of use.
5. Students and employees must comply with all applicable laws, including those relating to copyrights and trademarks, confidential information, and public records. Any use that violates state or federal law is strictly prohibited.
6. Users may not install or use any internet-based file sharing program designed to facilitate sharing of copyrighted material. Plagiarism of internet resources will be treated in the same manner as any other incidents of plagiarism.
7. No user of DCS technology resources, including a person sending or receiving electronic communications, may engage in creating, intentionally viewing, accessing, downloading, storing, printing, or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages, or other material that is obscene, defamatory, profane, pornographic, harassing, abusive, or considered to be harmful to minors.
8. No user shall use DCS technology resources to cyberbully, threaten, demean, or otherwise emotionally or mentally harm another student or employee.
9. Schools may not change the Internet Usage or Acceptable Use agreement forms.
10. The Acceptable Use Agreement and Portable Device Agreement forms must be signed by parents every year during the first 2 weeks of attendance or students may be delayed in using DCS technology resources and receiving their district-issued Chromebook.
11. The DCS School District will not be responsible for any data or network related issues users may experience such as loss, damage, or unavailability of data stored on or transmitted through DCS technology resources as well as network delays, changes, or interruptions of service.
12. Student social media use is blocked by filtering policies on the DCS network. Some social media may be used by the DCS District to communicate with the public. High school students are allowed to use Twitter during the instructional day for educational purposes only. DCS is not responsible for student social media access using personal devices.

Educational Applications

DCS utilizes Google-based learning applications such as Google Classroom, Google Docs, Google Slides, and other Google learning services. These tools allow teachers and students to work collaboratively on assignments and allows our students immediate access to their work, from any device, be it a smartphone, tablet, laptop, Chromebook or desktop computer. DCS utilizes age-appropriate legal and ethical guidelines in order to protect students and staff from data and identity security violations.

Other online learning tools are used for classroom education. These additional apps, extensions and educational websites are vetted and approved by district and school staff prior to use. Parent signatures are required for use of age-restricted applications. More information can be found on the DCS district [website](#).

Filtering and Monitoring

DCS takes reasonable precautions in accordance with CIPA and COPPA guidelines by using filtering software to keep inappropriate internet websites and email out of the classroom. However, it is recognized that this filter alone is no guarantee that users will not be able to find internet resources which are profane, offensive, obscene, or otherwise objectionable. As much as possible, technology resources should direct students to those resources which have been evaluated prior to use. Staff should provide supervision during all internet activities.

All district employees and students are expected to report any system misuse, inappropriate internet sites that are not stopped by the district's internet filter, and behavior that falls within the district's discrimination and sexual harassment policies

Google for Education

DCS provides all users access to a suite of web-based educational applications and tools called Google Workspace for Education (GWFE). These applications include word processing, spreadsheets, presentations, calendars, email, Google Classroom and other collaborative tools. These applications run on an internet domain purchased and owned by DCS and are intended for educational use. Students and teachers may utilize these tools for lessons, assignments, and communication. This suite of applications is available in "the cloud", which allows students immediate access to their work, from any device, be it a smartphone, tablet, laptop, or desktop computer and from any location such as school, home, public library or any other place with internet access.

In order to create a safe, effective way for students and staff to communicate with one another, DCS provides all users with a unique username and password which will be used for access to these applications and resources. No user data collected in the core services is used for advertising purposes, nor is user data sold to third-party companies. Service data collected is primarily used to deliver the services that schools and students use, but it's also used to maintain and improve the services; make recommendations to optimize the use of the services; provide support; protect our users, the public, and Google; and comply with legal obligations. For more information, see the [Google for Workspace for Education Privacy Policy](#).

Guidelines for use of Google Workspace for Education Plus:

1. Not all applications are used at all grade levels. Some applications are better suited to older students. Applications are restricted by age when necessary or legally required.
2. Users will have no expectation of privacy with their GWFE account, and thus should remain committed to using it academically and professionally.

3. Users should never share their passwords with anyone else; likewise, user's should never use anyone else's password. Users will not act in a way that jeopardizes the account security of another student or staff member.
4. Users should never use their GWFE account to promote any unlawful activities or personal financial gain.
5. Users will not post personal contact information about themselves or other people using their GWFE account.
6. Inappropriate language, personal insults, profanity, spam, racist, sexist or discriminatory remarks, or threatening comments will not be tolerated. Additionally, users should not use their account to promote or spread inappropriate or offensive content, or to threaten another student or staff member.
7. Students will inform a member of the district staff should they receive any message that is inappropriate or makes them feel uncomfortable; likewise, staff will inform their school administrator.
8. 6th thru 12th grade students may use their email address to register with various educational websites, and, consequently, be able to receive email messages from these websites. For grades 6th thru 8th, this will be more restrictive than the high school grades. Elementary grades are only allowed to email teachers and other elementary students. All email is monitored by district monitoring systems.
9. Student email is ad free, and is filtered for spam.
10. High school students cannot email middle or elementary students. Middle school students cannot email high school or elementary school students. Likewise, elementary students cannot email middle or high school students.
11. User email is archived internally, and is searchable by district administrators at any time, should the district deem it necessary.
12. Parents are responsible for monitoring their child's use of GWFE outside of school. Students are responsible for their own behavior at all times.
13. Access to, and the use of, GWFE is considered a privilege and benefit to users in the district. DCS maintains the right to immediately revoke this access and use of the GWFE learning applications where the district has reason to believe violations of law or district policy have occurred.



DICKSON COUNTY SCHOOLS Technology Acceptable Use Agreement

STUDENT

- ☐ I have read the information and guidelines outlined in this agreement and I agree to follow them.
- ☐ I agree to follow all Google for Education guidelines.

Student First Name (PRINT)

Student Last Name (PRINT)

Student Signature

Date

PARENT

- ☐ I have read the terms and conditions of this agreement and I agree to follow them.
- ☐ I give my child permission to utilize Google for Education learning tools.

Parent/Guardian First Name (PRINT)

Parent/Guardian Last Name (PRINT)

Parent/Guardian Signature

Date