# TRIMBLE COUNTY PUBLIC SCHOOLS

# Electronic Resources Acceptable Use Guidelines

## Access to Electronic Media

**Student, Staff, and Community Member Use**

Trimble County Public Schools (TCPS) support student, staff, and community access to all forms of educational technology and believe it is incumbent upon students, staff, and community members to use this privilege in an appropriate and responsible manner.

**Procedures and Guidelines**

The Superintendent or a designee  (currently the Trimble County District Technology Committee) shall develop and implement appropriate procedures to provide guidance for student, staff, and community member access to electronic media. Guidelines shall address ethical use of electronic media, including the Internet, issues of privacy versus administrative review of electronic files and shall prohibit use of the District's technology for unacceptable activities which will be described in this document.

**Permission/Agreement Form for Student and Parents**

All students who will utilize the District network (TCPSnet) will need to sign a Network Access Agreement. This form outlines acceptable use of TCPSnet and requires a parent signature. Parents may indicate whether they will permit student/school employee contact via texting and social media for school-related purposes.

This document shall be kept on file as a legal, binding document. In order to modify or rescind the agreement, the student's parent/guardian must provide the Superintendent with a written request.

**Agreement for Staff and Community Members**

School district employees and community members shall submit a signed agreement form prior to using District technology in an unsupervised setting.  This document shall be kept on file as a legal, binding document.

**Cyberbullying**

Students shall be provided instruction about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyberbullying awareness and response.

**General Standards - Users**

The following standards apply to student, staff, and community member access to electronic resources.

## Students

\* Students may access network resources using an individualized login (first.last@stu.trimble.kyschools.us.). Elementary schools sometimes prefer to use generic student logins line Student 1, Student 2 , etc. Individual logins allow students a district storage directory for student work. Student accounts also have data storage available through Microsoft and Google.

\* Students' access to the Internet should occur only under the direct supervision of a district employee.

**Students will have individual district-provided email accounts as required by KDE. Students using district devices will use web mail provided by the Kentucky Dept. of Ed.

## Certified and Classified Staff

*TCPS will create accounts for employees who need network access. The appropriate forms and training must be completed. Access is provided for educational and work related purposes only. Teachers and staff may not use TCPSnet for personal gain**.

Employees shall not use a code, access a file, or retrieve any stored communication or data unless they have been given authorization to do so as part of their duties. Each employee is responsible for the security of his/her own password.

## Audit of Use

The Superintendent/designee shall establish a process to determine whether the District's education technology is being used for purposes prohibited by law or for accessing sexually explicit materials. The process shall include, but not be limited to:

1. Utilizing technology that meets requirements of Kentucky Administrative Regulations and that blocks or filters internet access for both minors and adults to certain visual depictions that are obscene, child pornography, or, with respect to computers with Internet access by minors, harmful to minors;

2. Maintaining and securing a usage log; and

3. Monitoring online activities of minors.

## TEXT MESSAGING, INSTANT MESSAGING, AND SOCIAL MEDIA

Employees, contractors, volunteers, and other adults working directly with students enrolled in the District shall not use text messaging services, instant messaging services, or social media sites (regardless of whether or not the equipment utilized for these purposes is owned by the District) to contact or communicate with students regarding school-related matters except in a manner consistent with Board policy. These individuals who wish to use text messaging services, instant messaging services, or social media sites to communicate with students regarding a class, club, team, activity, or event must submit a statement to the principal/designee of the school the student attends to briefly describe the purpose of the intended use of text messaging, instant messaging, or social media in the context of the class, club, team, activity, or event. Each student who wishes to participate in the exchange of text messaging, instant messaging, or social media for the class, club, team, activity, or event, must obtain written consent from a parent/legal guardian.

District employees and activity sponsors may set up blogs and other social networking accounts using District resources and following District guidelines to promote communications with students, parents, and the community concerning school-related activities and for the purpose of supplementing classroom instruction.

Networking, communication, Office 365, Google and other options offering instructional benefits may be used for the purpose of supplementing classroom instruction and to promote communications with students and parents concerning school-related activities.

In order for District employees and activity sponsors to utilize a social networking site for instructional, administrative or other work-related communication purposes, they shall comply with the following:

1. They shall request prior permission from the Superintendent/designee.

2. If permission is granted, staff members will set up the site following any District guidelines developed by the Superintendent's designee.

3. Guidelines may specify whether access to the site must be given to school/District technology staff.

4. If written parental consent is not otherwise granted through AUP forms provided by the District, staff shall notify parents of the site and obtain written permission for students to become "friends" prior to the students being granted access. This permission shall be kept on file at the school as determined by the Principal.

5. Once the site has been created, the sponsoring staff member is responsible for the following:

    a. Monitoring and managing the site to promote safe and acceptable use; and

    b. Observing confidentiality restrictions concerning release of student information under state and federal law.

Staff members are discouraged from creating personal social networking sites to which they invite students to be friends. Employees taking such action do so at their own risk.

No employee, contractor, volunteer, or other adult working directly with students enrolled in the District shall engage in any sexually related behavior with a student utilizing electronic communications, including but not limited to sexual jokes; sexual remarks; sexual kidding or teasing; sexual innuendo and pressure for dates or sexual favors.  If an employee, contractor, volunteer, or other adult working directly with students enrolled in the District utilizes a student's telephone number, email address, or user/screen name on a messaging services or social networking site, which was obtained from school records, for a purpose inconsistent with Board policy, such use constitutes a misuse of personally identifiable information or educational records, and may result in discipline, up to possible termination of employment.

All employees shall be subject to disciplinary action if their conduct relating to use of technology or online resources violates Board policy or other applicable policy, statutory or regulatory provisions governing employee conduct. The Professional Code of Ethics for Kentucky School Certified Personnel requires certified staff to protect the health, safety, and emotional well-being of students and confidentiality of student information. Conduct in violation of this Code, including, but not limited to, such conduct relating to the use of technology or online resources, must be reported to Education Professional Standards Board (EPSB) as required by law and may form the basis for disciplinary action up to and including termination.

**Software**

Students are not allowed to put software on any district computing device.

**Students are not allowed to access any website or software application that blocks, mitigates or bypasses the security and monitoring software that have been installed by the district Technology Department.**

Each teacher is responsible for providing proof of ownership of all software installed on his/her computer which was not purchased by the school or the district.

## Privacy, rights, and responsibilities

The superintendent (or a designee), the Chief Information Officer, the Network Administrator, and the principals (within their respective buildings) have the right to access information stored in any user directory, on the current user screen, or in electronic mail. Users are advised not to store personal confidential data. While the District retains the right to access all user accounts and stored information, the District will access this information only for maintenance, security purposes, or where there is a compelling reason.  Network management and monitoring software will be used to insure compliance with all applicable district policies and with state and federal legislation. Specifically, Senate Bill 230 requires all Kentucky school districts to restrict access to sexually explicit and other questionable material on the Internet and to audit Internet usage to insure that employees and students honor the restrictions. Trimble County Schools will comply with SB230 and take appropriate action when policies are violated.

## Network and Internet Policies

Access to all electronic resources at Trimble County Public Schools is a privilege and carries with it responsibilities. The following general policies apply to all users.

1. Trimble County Public Schools maintain the right to limit access to software and/or documents found on the Internet.

2. Trimble County Public Schools will not be responsible for damages caused by loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions for any reason.

3. Security on any computer system is a high priority, especially when the system involves many users. If any user identifies a security problem on TCPSNet, s/he must notify the Technology Department and should not demonstrate the problem to other users.

4. Vandalism shall result in cancellation of privileges. Vandalism is defined as any attempt to harm or destroy data, hardware or software of TCPSNet or any agencies or other networks that are connected to KETS Internet backbone.  Vandalism includes altering any settings on any district computer or installing any unauthorized software, utilities, or games.

Violation of the following terms and conditions  may result in the immediate loss of network services.  The use of your account must be in support of education and consistent with the objectives of the Trimble County Schools.

* You may not give your password to anyone.

* You may not use or alter anyone else's Internet network account.

* You may not offer Internet access to any individual via your TCPSNet account.

*You may not purposefully visit Internet sites that are sexually oriented or those that promote violence, hate, racism, or discrimination. Nor will you purposefully visit sites that provide information about any activity intended to lead to personal injury or property destruction. Trimble County Schools provide Internet access for educational purposes; therefore, the classroom teacher will decide whether a specific Internet site meets his/her educational goals if there are questions of appropriateness.

* You may not break in or attempt to break into other computer networks.

* You may not create or share computer viruses.

* You may not destroy another person's data.

* You may not monopolize the resources of TCPSNet by such things as running large programs and applications over the network during the day, or using system resources for games.

* You are not permitted to get from or put onto the network any copyrighted material (including software, images, and digital music)

*No form of instant messaging or chatting is to be used on TCPSnet without permission.

* As a user of this community system, users should notify the Technology Department of any violations of this contract taking place by other users or outside parties. This may be done anonymously.

* No illegal activities may be conducted via the network

* All communications and information stored on the network should be assumed to be the private property of Trimble County Public Schools.

* Acceptable Use of other organizations' networks or computing resources must comply with the rules appropriate for that network. Transmission or storage of any material in violation of any U.S. or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret.

**Electronic Mail Regulations**

*Email should pass two tests:

> (1)Does it lead to personal gain for the sender?  If so, don't send it.

> (2)Is it educational or work related?  If not, don't send it.

Community announcements may be sent with the best intentions but if they can't pass the test, don't send them.

Email users should consider chain of  command when sending email to groups.  In most cases, only those who supervise whole buildings/departments/entities should send to the whole group.  That is, principals (and some central office personnel) generally speaking will be sending emails to a whole school; others should consult with the principal if there is any doubt about the appropriateness of a school-wide email.  The same is even more important at the district level.  Only the superintendent and a few central office personnel should send to the whole district. Principals should consider appropriateness before sending to all users at another school.  NO ONE AT TRIMBLE COUNTY SCHOOLS SHOULD SEND TO ALL USERS AT ANOTHER DISTRICT OR TO ALL USERS IN THE STATE.

**\***Students should use personal distribution lists judiciously. Complaints from other users may result in the loss of  email privileges.

*Each TCPSnet user has only one acceptable method of using email…that is the district provided email account.  No other internet mail is approved for use.

*Do not forward or send chain messages, "public service announcements", or any non-instructional communication – especially to entire schools, districts, or departments.

* Be polite. Do not write or send abusive messages to others.

* Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.

* Students must not reveal personal addresses or phone numbers

* District email is provided by Microsoft through Office 365.  We rely on MS for the maintenance of email backups.

* Note that 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. For additional information see board policies found in the Student Code of Conduct (BP 9.438) and in BP 03.1321, BP 03.2321, BP 03.2325, and BP 03.1325 for certified and classified employees regarding use of school property, disrupting the educational process, and conduct.

**Loss of Network Services**

The superintendent or a designee may suspend or close an account at any time as required. Revocation of network privileges will be for a period determined by the appropriate building level administrator. Users (students, staff, or community members) whose accounts are denied, suspended or revoked may:

1. Request (in writing) from the district a written statement justifying the actions.

2. Submit a written appeal to the Superintendent.

3. Appeal to the board of education. The decision of the board of education is final.

Faculty and Staff who knowingly and deliberately violate Board policy, may be subject to an official reprimand by their immediate supervisor and can be reported to the Superintendent for more severe job action or termination if the nature of the violation warrants.

**RESPONDING TO CONCERNS**

School officials shall apply the same criterion of educational suitability used to review other educational resources when questions arise concerning access to specific databases or other electronic media.

# TCPS Employee Internet Network Access

I have read the Trimble County Schools electronic resources Acceptable Use Guidelines and agree to follow the acceptable use of the network and proper network etiquette.   My signature below indicates that I agree to follow the guidelines.  I understand that I am responsible for my own personal behavior using Trimble County Public Schools electronic resources.

Employee Name (please print): _____

Employee Signature: _____

School/Location: _____ Date:____/____/____School Year: _____

This document is to be kept on file by the School Building Technology Coordinator or Chief Information Officer

**Text messaging, Instant Messaging, and Social Media – TEACHER Registration For Use**

Employees, contractors, volunteers, and other adults working directly with students enrolled in the District wishing to use text messaging services, instant messaging services, or social media sites to communicate with students regarding a class, club, team, activity, or event must utilize this form or submit the information required by this form on a separate paper or electronically to the principal(s) of the school(s) where the students attend who are involved in the class, club, team, activity, or event.

Name of class/club/team/activity/event: _____

Name of employee/contractor/volunteer/other adult: _____

Specific type/method of communication: _____

(text messaging/instant messaging/social media site)

Description of how use of this type/method of communication will be utilized in the class/club/team/activity/event identified above:

_____

_____

_____

_____

_____

_____

I acknowledge my use of electronic communications with students in relation to a class/club/team/activity/event is governed by Board Policy 08.2323, and that I may not use contact information regarding a student gained from school records to communicate with a student for a purpose inconsistent with Board Policy 08.2323.

I have read the Trimble County Schools electronic resources Acceptable Use Guidelines and agree to follow the acceptable use of the network and proper network etiquette.  My signature below indicates that I agree to follow the guidelines.  I understand that I am responsible for my own personal behavior using Trimble County Public Schools electronic resources.

Teacher/Staff Name (please print):
_____

Teacher/Staff Signature:
_____

School/Location: _____ Date:____/____/____School Year: _____

------ This document is to be kept on file by the School Building Technology Coordinator. --------

**TEXT MESSAGING, INSTANT MESSAGING, AND SOCIAL MEDIA – PARENT PERMISSION FORM**

Employees, contractors, volunteers, and other adults working directly with students enrolled in the District wishing to use text messaging services, instant messaging services, or social media sites to communicate with students regarding a class, club, team, activity, or event must obtain parent/guardian permission (for students who are under 18 years of age) utilizing this form.

Name of class/club/team/activity/event: _____

Name of employee/contractor/volunteer/other adult: _____

Student's name: _____

I give permission for the above-named employee to contact my student by text messaging/instant messaging/social media for the class/club/team/activity/event identified on this form consistent with Board Policy 08.2323 using the contact information below.

Cell phone number authorized for student contact: _____

Instant messaging program/screen name for student contact: _____

Social media (i.e., Facebook, Myspace, etc.) site/screen name for student contact: _____

_____

_____          _____

Parent/Guardian Signature                                            Date

_____

Parent/Guardian name (printed)

# Guidelines for Teacher and Student Owned Computers

Board Policy and these guidelines must be interpreted within the framework of all other school and district precedures that set guidelines, restrictions, and prohibitions on the use of digital devices. This includes telecommunications devices. It is increasingly difficult to categorize digital devices; Principals will make the final decision if there is disagreement on the use of any digital device.

The Trimble County School District appreciates the fact that employees and students are willing to bring in personally owned computer equipment to be used for schoolwork and student use. However, several items must be addressed when connecting a non-KETS standard device to the district network.

1. Overview
2. Software
3. Support
4. Conditions
5. TCPS Rights
6. Acceptance

## *Overview*

- A student or employee who brings privately owned computers/other technology devices to school is personally responsible for the equipment. Responsibility for the maintenance and repair of the equipment rests solely with the student/staff member. Any damage to the equipment is the responsibility of the individual. Any device that is capable of interfacing with the district network is considered a computer.

## *Software*

- Software residing on private computers must be personally owned. All devices must include anti-virus software as necessary. The student or employee will be responsible to provide proof of this information upon request

## *Support*

- District technicians will not service, repair, support, or setup any computer not belonging to the district. No internal components belonging to the district shall be placed in any personal equipment, whether as an enhancement, upgrade or replacement. No software that is installed on a personal machine will be supported by district level personnel. If personal software interferes with the district network software or hardware, a technician WILL remove the computer from the network until such time that said computer is compatible with our network settings. Any damage caused by use in the Trimble County School District is the responsibility of the owner.
- Technology peripherals (printers, scanners, projectors, etc.) purchased privately to be used in the school system must also be maintained by the owner. Purchasing perishable supplies to be used in equipment not owned by the district is the owner's responsibility.

## *Conditions*

A privately owned computer can be connected to the district's network, including access to the Internet, under the following conditions:

- Use of the device must adhere to Board Policy
- The individual must supply all necessary hardware/software and cabling to connect to the network. The technology department will provide a guest wireless network connection for the device to connect to.
- Privately owned computers must be running current virus detection software prior to accessing the network or Internet. If no anti-virus program is installed, there are several available on the internet for free download.

## *TCPS rights*

- The district retains the right to determine where and when privately owned equipment may connect to the network. The student/employee is responsible for the security of the equipment at all times. Trimble County School District does not guarantee the privacy or security of any item(s) stored on or transmitted by any privately owned computers.
- For privately owned computers being used in district facilities, the Trimble County School District reserves the right to:

  1. Monitor all activity.
  2. Make determinations on whether specific uses of the computer are consistent with Board Policy.
  3. Log network use and to monitor storage disk space utilized by such users.
  4. Deem what is appropriate use.
  5. Remove the user's access to the network and suspend the right to use the privately owned computer in district facilities if at any time it is determined that the user is engaged in unauthorized activity or is violating Board Policy.
  6. Devices with cellular or other internet access not provided by the district are still bound by all the provisions of Board policy and the use is subject to the authority of district employees.  Students may not violate any part of these guidelines simply because they are using a paid cellular data plan.

***Students must not connect to any wireless network that is not owned by the district while they are on school grounds.***