TRUSD Technology Use Agreement – Student

Overview and Purpose

Twin Rivers USD provides Internet access to all students and staff. Internet access allows classrooms and individuals to have access to information, software, news and opinion, and communication by electronic mail that originates from any point in the world. All users must agree to the guidelines in this Code of Conduct to have access to the Internet through their classrooms, library, or computer labs.

Our network system has been established for educational purposes including classroom activities, direct and independent learning activities, individual and collaborative writing and publishing, career development, personal productivity, and other high-quality learning activities. Our district has the right to place reasonable restrictions on the students who can access the network system and the material they may post on the network system. All users shall not hold the District or any District staff responsible for the failure of any technology protection measures, violations of copyright restrictions, or users' mistakes or negligence. All users shall agree to indemnify and hold harmless the District and District personnel for any damages or costs incurred.

Limitations of Liability

Personal Gain

The TRUSD network may not be used for commercial purposes, financial gain, personal business, product advertisement or political lobbying activities. Advertising on district or school web sites may be accepted under the same restrictions and conditions set forth in law, Board policy, and administrative regulations pertaining to advertising in district and school-sponsored publications (BP 1113).

Personal Safety

Students should not post personal contact information about themselves or other people on the TRUSD network. Personal contact information includes one's full name, address, telephone number, school address, work address, etc. No student should agree to meet with someone he or/she has met online without parent/guardian approval.

Unauthorized Access

No students will attempt to gain unauthorized access to the TRUSD network or go beyond authorized access. This includes attempting to log on through another person's account or access another person's files. No student will attempt to disrupt the TRUSD network system or destroy data by spreading computer viruses or by any other means. No student may use the TRUSD network to engage in any illegal act, such as arranging for a drug sale, engaging in criminal gang activity, threatening the safety of another person, and engaging in gambling activities.

Individual Accounts

Each individual user is responsible for his or her individual account and should not provide his or her password to another person. All individual users will avoid the inadvertent spreading of computer viruses by following the district virus protection procedures when downloading software. Large files may not be downloaded unless absolutely necessary. If necessary, a student will download the file only with the permission from the teacher in authority.

Spamming

Students will not post chain letters or engage in spamming. Spamming is defined as sending an unsolicited message to an individual or a group of people.

Network Vandalism

Vandalism is not permitted and will be strictly disciplined. Vandalism is defined as any attempt to harm or destroy data of another user or of another agency or network that is connected to the Internet or Intranet (District internal network). Vandalism includes, but is not limited to, the uploading, downloading, or creation of computer viruses, logic bombs, ASCII mail bombs, Trojan horse programs, or any software utilized to scan the network for passwords or confidential information.

Online Communities & Communications

While many sites and online communities and communications are accessible as educational tools within TRUSD classrooms, some are deemed inappropriate and are blocked within the TRUSD network. Various online communities may be used for educational purposes including but not limited to: google suite, wikis, blogs, social networks (e.g. schoolology), video/photo sharing sites (e.g. youtube), virtual classrooms/chat areas (e.g. School Loop), video conferencing, and discussion boards. TRUSD reserves the right to block network access to any online resources at any time. Any links to external webs sites shall support the educational mission and shall include a disclaimer that the district is not responsible for the content of the external web sites (BP 1113).

The following restrictions apply to all types of online communities and communications utilized within the TRUSD network:

Inappropriate Language

Restrictions against inappropriate language apply to public messages, private messages, and material posted on TRUSD Websites. In general, users should make language choices which are appropriate for school situations. Students may not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language when using the TRUSD network. Students may not engage in personal attacks, including prejudicial or discriminatory attacks against another individual through the use of the TRUSD network.

Inappropriate Materials

No student may use the TRUSD network to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people. If an individual user mistakenly accesses inappropriate information, he or she should immediately tell his or her administrator.

Possession and Use of Personal Technology

Users may possess or use personal technologies on campus (e.g. cell phones) provided that such devices are not used for illegal or unethical activities such as cheating on assignments or tests. All such student devices may be used only at the teacher's discretion for instructional purposes only (BP 5131). Students should under no circumstances record or photograph others without their expressed consent. This includes publishing or posting such material online. Users who misuse or aid in the misuse of personal technology "may be prohibited from possessing a mobile communications device at school or school-related events and may be subject to discipline in accordance with Board policy and administrative regulation (BP 5131).

Use of Student Image & Student Work

Photographs of students with their names may be published EXCEPT when the student's parent/guardian has notified the district in writing to not allow the release of the student's photograph without prior written consent (BP 1113).

Cyberbullying, Harassment & Discriminatory Attacks

TRUSD Governing Board Policy 5131 defines "Student Disturbances" as: "Harassment of students or staff, including bullying, intimidation, so-called "cyberbullying," hazing or initiation activity, ridicule, extortion, or any other verbal, written, or physical conduct that causes or threatens to cause bodily harm or emotional suffering. Cyberbullying includes the posting of harassing messages, direct threats, social cruelty, or other harmful text or images on the Internet, social networking sites, or other digital technologies, as well as breaking into another person's account and assuming that person's identity in order to damage that person's reputation or friendships."

Cyberbullying conducted using district-owned equipment or on school premises, as well as off-campus cyberbullying that impacts school activity or school attendance, may be subject to discipline in accordance with district policies and regulations. If the student is using a social networking site or service that has terms of use that prohibit posting harmful material, the Superintendent or designee also may file a complaint with the Internet site or service to have the material removed. Students are encouraged to save and print any messages sent to them that they feel constitutes cyberbullying and to notify a teacher, or other employee so that the matter may be investigated (BP 5131).

Online Academic Dishonesty

The TRUSD Board of Trustees believes that academic honesty and personal integrity are fundamental components of a student's education and character development. The Board expects that students will not cheat, lie, plagiarize or commit other acts of academic dishonesty. (BP 5131.9)

Online Cheating

Examples of misuse include, but are not limited to: taking an online test for another student, using cell phones or email with the purpose of distributing answers, and "hacking" into a teacher's computer or gradebook.

Online Plagiarism

Submitting another student's work as your own, knowingly using or building upon an others ideas without proper citation, and using the internet to purchase or find a paper are all acts of plagiarism. This applies not only to written work, but to any school project for which technology is used as a research tool or method of presentation (e.g. Power Point presentations, wiki's, etc.).

Copyright Infringement

If a work contains language that specifies appropriate use of that work, students should follow the expressed requirements for citing the work. If unsure whether or not one can use a work, one should request permission from the copyright owner.

Student Signature	Date
•	
Parent/Guardian Signature	Date