Student Technology Use Guidelines

Student Technology Use Guidelines 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

District technology may not be used for commercial purposes, financial gain, personal business, product advertisement or political lobbying activities. Advertising on District or school websites 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 Identifiable Information (PII) about themselves or other people on the TRUSD network. PII includes one's full name with other information that would allow an individual to locate you, including, but not limited to, your parent's name, your home address or location, your telephone number, your school address or location, your work address or location, your email address, or your website or social media page(s). Students should not agree to meet with someone he/she has met on- line without parent/guardian approval. You will not disclose names, personal contact information, or any other private or personal information about other students under any circumstances. You will not forward a message that was sent to others privately without permission of the person who sent the message.

Unauthorized Access

No students will attempt to gain unauthorized access to TRUSD network or to any other computer system while using district technology, or go beyond your authorized access. This includes attempting to log on through another person's account. No person may use any device or software to gain

unauthorized access to another person's files or private information. No student will make deliberate attempts to disrupt the TRUSD network system, or any other computer system, or destroy data by spreading computer viruses or by any other means, or attempt to obtain another student's logon information. No student may use district technology 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 material. Large files may not be downloaded unless absolutely necessary and 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 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 use of viruses, key- logging tools/software, Trojan horse programs, or any software utilized to scan the network for confidential information or bypass security measures put in place by the district.

Online Communities and 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 Apps for Education, wikis, blogs, social networks, learning management systems, internal communication systems, 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 websites shall support the educational mission and shall include a disclaimer that the district is not responsible for the content of the external websites (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 all speech communication while using district technology, including but not limited to, public messages, private messages, and material posted on webpages. 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 district technology. Students will not post information that could cause damage or a danger of disruption using district technology. Students may not engage in personal attacks, including prejudicial or discriminatory attacks against another individual through the use of district technology. Students will not harass another person using district technology. Harassment is persistently acting in a manner that distresses or annoys another person. If you are told by a person to stop sending them messages, you must stop. Students will not knowingly or recklessly post false or defamatory information about a person or organization using district technology.

Inappropriate Materials

No student may use district technology to access material that is profane or obscene (pornography), material that has been designated as for "adults" only, and material 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 teacher or school 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 (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)

A student's possession or use of a personal electronic device (including a cell phone) on school grounds constitutes the student's specific consent to the search by a school official of the student's personal electronic device when there is a reasonable suspicion that the search will uncover evidence that a student is violating the law, Board Policy, or other rules of the district or the school (E 6163.4)

In the case of district technology, there should be no assumption of privacy or confidentiality. The district reserves the right at any time to review all content on and sent from district systems and devices. It is a public asset that should only be used in the pursuit of learning and education opportunities.

Use of Student Image & Student Work

Photographs of students with their names may be published by the district 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. (BP1113)

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 technology 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 or test questions, and "hacking" into a teacher's computer or grade book.

Online Plagiarism

Submitting another student's work as your own, knowingly using or building upon another's 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. PowerPoint presentations, wikis, etc.).

Copyright Infringement

lf 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_____