Internet/Network/Email - Terms and Conditions of Use

Students are responsible for good behavior on the school district computer networks and email accounts, just as they are in a classroom or on a school campus. General rules and policies for behavior and communications in the district apply. Users are subject to all local, state and federal laws. Illegal activities are strictly forbidden.

The network and email accounts are provided for students to conduct research and communicate with others. They are to be used for educational and other school related uses only. Access is a privilege - not a right, and is given to students who agree to act in a considerate and responsible manner. Access entails responsibility. Inappropriate use will result in a suspension or cancellation of privileges and may also result in other penalties. Authorized personnel may close an account at any time as warranted. The administration, faculty and staff may also request authorized personnel to deny, revoke, or suspend specific user accounts.

Users are expected to abide by generally accepted rules of network and email etiquette

1. Be polite. Do not send abusive messages to others.
2. Use appropriate language. Do not use obscene, profane, lewd, vulgar, disrespectful,
3. threatening or inflammatory language or swear, use vulgarities or any other inappropriate language. Harassment and personal attacks, including the use of prejudicial, discriminatory, racist or sexist language, are prohibited.
4. Do not reveal personal information such as name, age, addresses, telephone numbers, or location, and do not reveal such information about others, except in District staff approved, protected situations. We encourage the responsible use of an online user identity.
5. Do not repost or forward personal communications without the sender’s consent.
6. Do not use the network or email messages in a way that disrupts the use of the network by others. Abuse of resources is prohibited, such as the sending of annoying or unnecessary messages to a large number of people or other functions that might restrict or interrupt data flow.

Users are not permitted to use computing resources for personal gain or commercial purposes, including advertising or purchasing products or services, political
lobbying or campaigning, promoting personal or religious ideas or causes, or inciting action by others.

Users are not permitted to transmit, receive, submit or publish any defamatory, prejudicial, discriminatory, abusive, obscene, profane, sexually oriented, threatening, offensive or illegal material. Students should not knowingly transmit, submit or publish inaccurate material. Students should notify school officials of any known infractions.

Any attempt to harm, alter, or destroy data of another user or any data on the network or related systems or agencies is prohibited. This includes, but is not limited to, the uploading, emailing or creation of computer viruses.

Damaging or altering computer systems or related hardware is prohibited. This can include installing or removing software/hardware without authorization. Electronic tampering with computer resources is not permitted. Gaining or attempting to gain unauthorized access to computers, networks, email accounts, files or data may result in cancellation of privileges and/or further disciplinary and/or legal action.

Users must comply with all licensing and copyright laws. This includes the use of audio/video/graphics/software/text as well as the use of media distribution systems such as SAFARI, ETR, and CCTV. Copyright guidelines are available at every school library media center; misuse or plagiarism in any form will not be tolerated.

Security on any network system is a high priority, especially when the system involves many users. Users are prohibited from giving out passwords, using someone else’s password, or impersonating other users on the network, Internet or email system. If you think you can identify any security problem on the district’s computers or networks, you must notify authorized personnel or a school official. Do not demonstrate the problem to others. Security infractions may result in cancellation of privileges and/or further disciplinary action.

Although electronic communication and information is generally treated as private property, users on the district network do not have personal rights of privacy in anything they create, receive, send, or store on or through the network, on district computer systems, or through district- provided email accounts. Authorized personnel (which may include a student’s parents or legal guardians) may review files and documents to maintain system integrity and ensure that users are using the system responsibly. The principal or
designee also may review files, documents, email, or communication forums. Documents, files or emails related to or in support of illegal activities may be reported to the authorities.

Web pages placed on the school network and/or Web server must be reviewed by authorized personnel to ensure that they adhere to the student code of conduct and the Guidelines for Thompson School District Web sites. Unauthorized access to and/or altering of web sites may result in disciplinary and/or legal action.

Users are not permitted to use Internet chat rooms or instant messaging because of the potential danger to users and to network security. To protect student and system privacy and safety, it is a violation for anyone to directly access an Internet chat room through any Thompson School District computer unless specifically assigned by a teacher. Should anyone unintentionally enter a chat room site or encounter inappropriate content, he/she must immediately disconnect from that site and report the information to a teacher. Use of specific instructional Internet or network conferences through First Class or other closed, teacher-monitored environments are permitted.

Student participation in non-teacher initiated and moderated instructional use of blogs, wikis, social networks, games or other interactive electronic environments is prohibited.

Any violation of this policy will result in serious consequences which may include loss of computer privileges up to one year, dismissal from computer related classes, loss of all Internet/network and/or email access, a temporary ban from computer labs, and/or other consequences imposed by school district policies and/or local, state or federal law, where applicable.