Tunica County School District

Technology Department

"Our Focus is Teaching and Learning"

Acceptable Use Policy

Tunica County School District
Acceptable Use Policy

INTERNET ACCESS

Tunica County School District (TCSD) provides the privilege of Internet access to district faculty, staff, students, and occasionally guests. Each user, as well as a minor's parent or guardian, voluntarily agrees to release, hold harmless, defend, and indemnify, the Tunica County School District, its officers, board members, employees, and agents, for and against all claims, actions, charges, losses or damages which arise out of the user's use of the TCSD network, but not limited to negligence, personal injury, wrongful death, property loss or damage, delays, non-deliveries, mis-deliveries of data, or service interruptions. TCSD will fully cooperate with local, state or federal officials in any investigation related to illegal activities conducted through the user's Internet account.

Access will be restricted as required to comply with the Children's Internet Protection Act. Web browsing may be monitored and records retained to ensure compliance.

Users are expected to respect the web filter and shall not attempt to circumvent the filter when browsing the Internet. The determination of whether material is appropriate or inappropriate is based solely on the content of the material and the intended use of the material, not on whether a website has been blocked or not. If a user believes a site is unnecessarily blocked, user should submit a technology work order to review the site.

Each user acknowledges that the information available from other websites may not be accurate. Use of any of the information obtained via the Internet is at the user's own risk. Tunica County School District makes no warranties of any kind, either expressed or implied, regarding the quality, accuracy or validity of the data on the Internet.

TCSD NETWORK RULES

- The person to whom an TCSD network account is issued is responsible at all times for its proper use.

- Any inappropriate use may result in the cancellation of the privilege of use, and/or disciplinary action. Consequences for any user who fails to comply with TCSD and school guidelines may include paying for damages, denial of access to technology, detention, suspension, expulsion or other remedies applicable under the school disciplinary policy, and state or federal law.

- Any district employee who uses the TCSD network inappropriately is subject to disciplinary action, including dismissal.

- Under no conditions should a TCSD network user give their password information to another user nor allow another user to utilize their account unless speaking directly to a technology department employee who is assisting them.

- Schools may supplement any provisions of the District AUP (Acceptable Use Policy), and may require additional parent releases and approvals, but in no case will such documents replace the District AUP.

- Users will immediately report to school district authorities any attempt by other network users to engage in inappropriate conversations or personal contact.

- Any non-standard software that is needed to perform a specific job function will need to be brought to the attention of the Technology Department. Those applications shall be the sole responsibility of that office and if the application interferes with any required programs, applications, and utilities, it should not be used and if in use, it may be disabled.

ACCEPTABLE USES OF TECHNOLOGY (not all inclusive)

A responsible user of the technology will:

- Use school technologies for school-related activities.

- Follow the same guidelines for respectful, responsible behavior online that they are expected to follow offline.

- Treat school resources carefully and alert staff if there is any problem with their operation.

- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.

- Alert a teacher, administrator, or other staff member if they see threatening, inappropriate, or harmful content (images, messages, posts) online.

- Use District technologies at appropriate times, in approved places, for educational pursuits.

This is not intended to be an exhaustive list. Users should use their own good judgment when using TCSD technology.

UNACCEPTABLE USES OF THE TECHNOLOGY (not all inclusive)

- Violating any state and/or federal law (i.e., copyright laws).

- Using profanity, obscenity, or other language that may be offensive to others.

- Making personal attacks on other people, organizations, religions, or ethnicities.

- Accessing, downloading, storing, or printing files or messages that are sexually explicit, obscene, or that offend or tend to degrade others. The administration invokes its discretionary rights to determine such suitability.

- Not respecting the privacy of a person by posting personal contact information, such as work/home address, telephone, e-mail, photographs, or names, without obtaining prior permission from the person affected.

- Student information shall be posted only with written parent/guardian permission.

- Forwarding personal communication without the author's prior consent.

- Using the Internet for commercial purposes, financial gain, personal business, producing advertisement, business service endorsement, or religious or political lobbying is prohibited.

- Destroying or altering the files of another user.

- Viewing or taking the files of another user.

- Using software or other tools (VPN or Proxies) to get around content filter.

FILTERING

An Internet filter is in place for Tunica County School District. This filter is a critical component of the TCSD network as well as Children's Internet Protection Act (CIPA) compliant since it allows valuable online Internet access while restricting access to specific unwanted material in the following categories:

- Pornography
- Gambling
- Illegal Drugs
- Online Merchandising
- Hate Speech
- Criminal Skills
- Alternative Journals
- Other Undesirable Materials

This filter is updated on a daily basis in order to restrict access to the above items. Filtering is not a 100% foolproof way of limiting access to appropriate sites. Inappropriate sites are added to the Internet daily. Students will be supervised at all times by a teacher while using the Internet. All inappropriate hits are logged along with the date/time and the IP address of the workstation making the request.

Attempts to bypass the school Internet filters is in violation of this acceptable use

policy and will be subject to disciplinary action that may include denial of access to technology, detention, suspension, expulsion, termination of employment or other remedies applicable under the school disciplinary policy, and state or federal law.

WORKSTATION MONITORING

All data transferred and/or transmitted over the TCSD network can be monitored and recorded at any time. All data transferred or transmitted over the network can be tracked and identified, and originating users can be held liable if their use of the network violates any established policy, regulation, or law. Any data stored on district-owned equipment may be archived and preserved by the district for an indefinite period. Such data includes, but is not limited to E-mail, text documents, digital photographs, music, and other digital or electronic files. If a particular workstation continues to try to connect to an inappropriate site, that workstation will be remotely monitored and the individual using that workstation will be reported to the Principal of the school and the TCSD Central Office.

TECHNOLOGIES COVERED

TCSD may provide the privilege or Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, email, and more.

The Acceptable Use Policy applies to both District-owned technology equipment utilizing the TCSD network, the TCSD Internet connection, and/or private networks/Internet connections accessed from District-owned devices at any time. This AUP also applies to privately-owned devices accessing the TCSD network, the TCSD Internet connection, and/or private networks/Internet connections while on school property or participating in school functions or events off campus. TCSD policies outlined in this document cover all available technologies now and in the future, not just those specifically listed or currently available.

USAGE POLICY

All technologies provided by the District are intended for education purposes. All users are expected to use good judgment by following the TCSD student code of conduct and social media policy. Users should be safe, appropriate, careful, and kind; should not try to disable or get around technological protection measures; use good common sense; and ask if they don't know.

EMAIL

Employee and student TCSD email is the property of TCSD. TCSD does not archive employee or student email. It is the responsibility of the employee and student to maintain this email account appropriately. However, TCSD has to right to seize and review the contents of email accounts if inappropriate activity is suspected.

<u>Use of outside email clients & stipulations for using district email client as district representative</u> (Teachers, Administrators, Managers, Students, etc.) Use of "Internet mail" by students, staff, and faculty such as Yahoo mail, Gmail, and POP3 accounts provided by their "home" Internet service providers is discouraged at this time. Viruses and malware can be downloaded to the network through outside email accounts.

The District does not block the use of Internet mail accounts, <u>but any "OFFICIAL" communications, e.g., Teacher to Parent, Teacher to Student, Staff to Staff, must be via the district's email system</u>. This includes, but is not limited to teachers who guide extracurricular activities such as Clubs, Choirs, Bands, Athletics, and the like.

SECURITY

Users are expected to take reasonable safeguards against the transmission of security threats over the TCSD network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. Users should never share personal information.

If users believe a computer or laptop they are using might be infected with a virus, they should alert the Technology Department. Users should not attempt to remove the virus themselves or download any programs to help remove the virus.

ONLINE ETIQUETTE

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.

Users should recognize that among the valuable content online there is also unverified, incorrect, or inappropriate content. Users should only use known or trusted sources when conducting research via the Internet.

Users should remember not to post anything online that they would not want students, parents, teachers, or future colleges or employers to see. Once something is online, it cannot be completely retracted and can sometimes be shared and spread in ways the user never intended.

PLAGIARISM

Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they did not create themselves, or misrepresent themselves as an author or creator of something found online.

Information obtained via the Internet should be appropriately cited, giving credit to the original author.

PERSONAL SAFETY

Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission. Users should recognize that communicating over the Internet brings anonymity and associated risks and should carefully safeguard the personal information of themselves and others. Users should never agree to meet in person someone they meet online without parental permission.

If users see a message, comment, image, or anything else online that makes them concerned for their personal safety or the safety of someone else, they should immediately bring it to the attention of an adult (teacher or administrator if at school, parent if using the device at home).

CYBER BULLYING

Cyber bullying including, but not limited to, harassing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking will not be tolerated. Users should not send emails or post comments with the intent to harass, ridicule, humiliate, intimidate, or harm the targeted individual and create for the targeted individual a hostile school environment.

Engaging in these behaviors or in any online activities intended to harm (physically or emotionally) another person, will result in disciplinary action. Responsible Use of the Internet and Cyber Bullying. In some cases, cyber bullying can be a crime. Users should remember that online activities might be monitored.

All students will be educated about appropriate online behavior, including interacting with other people on social networking websites and in chat rooms, and cyberbullying awareness and response.

SOCIAL MEDIA

The District has a policy that addresses Fraternization via Social Media, which applies to all employees and students. By signing the Acceptable Use Policy, users are acknowledging they have read and agree to abide by the Fraternization guidelines (**in Employee Handbook**).

Accessing academic and professional networking during school hours is allowed. Personal social networking is prohibited during school hours. Those employees who choose to utilize academic/professional and personal social networking should do so responsibly. Disclosure of confidential information is prohibited, regardless of when such a disclosure occurs. Inappropriate conduct on social networking sites could adversely affect the employee's ability to carry out the responsibilities of his or her job. Students are prohibited from Social Media during school hours.

Employees and students are prohibited from posting on any site inappropriate data,

documents, photos, or information that might result in a disruption of normal school operations. Fraternization, via social media, between employees and current K-12 students is prohibited. Teachers should not post K-12 students on personal social media outlets.

Social Media Pages
The school district maintains a Facebook page and Twitter account. The accounts are monitored and maintained by the Technology Department and designees. These social media outlets are meant to be a place for current students, parents, alumni, staff, and other district stakeholders to interact, ask questions and discuss topics relevant to TCSD. No Social Media pages should be created for schools, organizations, or school related activities without the written consent of the Superintendent of Education.

The District reserves the right to block individual accounts and/or remove comments, links, photos or other content from these social media sites for any reason, including but not limited to, harassment and personal attacks, derogatory or defamatory comments, vulgarity and profanity (including expletives and letters followed by dashes), commercial promotion, off-topic posts, improper use of intellectual property or copyrighted material, and all inappropriate content.

LIMITATION OF LIABILITY

TCSD will not be responsible for damage or harm to persons, files, data, or hardware.

While TCSD employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

TCSD will not be responsible or liable for, financially or otherwise, unauthorized transactions conducted over the TCSD network.

Violations of this policy may have disciplinary consequences, including:

- Suspension of network, technology, or computer privileges;
- Notification of parents;
- Detention or suspension from school and school-related activities;
- Employment disciplinary action up to and including termination of employment;
- Legal action and/or prosecution.

Employees, students, and parents/guardians shall be required to sign the District's Acceptable Use Policy as part of the district's Technology Handbook before Internet or network access shall be allowed.

USER AGREEMENT - STATEMENT OF RECEIPT

This form is to be completed by each user of the Tunica County School District Network and kept in the employee's file.

Name _____

Position _____

School or Department _____

I have read the District Acceptance Use Policy. I agree to follow the rules contained in this Policy. I understand that if I violate the rules my privilege of using the Internet can be terminated and I may face disciplinary action in accord with the Code of Ethics of the District Policies and Procedures. I hereby release the district and its personnel from any and all claims and damages of any nature arising from my use of, or inability to use, the Tunica County School District system, including, but not limited to claims that may arise from the unauthorized use of the system to purchase products or services. I understand that this form must be signed and renewed every year to maintain my network privileges.

Signature _____ Date _8/22/2019_