

# Tangipahoa Parish School System

## Technology Acceptable Use Policy (AUP)

The Tangipahoa Parish School Board believes it is necessary for all persons to become aware of acceptable use of computers. Any person using computers or other electronic information resources shall be required to use such equipment and resources in a responsible, legal manner. The School Board retains the right to monitor all computer usage and files for compliance to all regulations and/or procedures.

Technology, particularly Internet access, is available to students and employees in the Tangipahoa Parish School System. We are very pleased to bring access to these resources to our school system. Technology offers vast, diverse, and unique resources to students, teachers, and administrators.

Our goal in providing these resources to our students is to enhance innovative education for students through access to unique resources and collaborations. Furthermore, teachers will improve learning and teaching through research, teacher training, collaboration, and dissemination of successful educational practices, methods, and materials.

Guidelines are provided so that the technology users are aware of the responsibilities they are about to assume. Responsibilities include appropriate, efficient, ethical, and legal utilization of network resources. The student's and parent or guardian's signatures on the attached contract is binding and indicates that he/she has read the terms and conditions carefully and understands their significance. In addition, ALL employees must sign and adhere to the provisions of this acceptable use policy.

### **TERMS AND CONDITIONS**

1. **Acceptable Use** - Technology resources in our school system shall ONLY be used to support teaching and learning. By providing access to unique resources and opportunities for collaborative work, technology can enhance student performance.
2. **Privileges** - The use of technology is a privilege, not a right, and therefore inappropriate use may result in the cancellation of those privileges by the administrator in each school.
3. **Network Etiquette** - Users are expected to abide by the Tangipahoa Parish School System rules of network etiquette. These include, but are not limited to the following:
  - a. **ALL hardware and software purchases and installations should be approved by the Technology Department.**
  - b. All technology hardware and software resources purchased by TPSS are the property of the Tangipahoa Parish School System and are loaned to students and faculty for their use.
  - c. Streaming or downloading media directly related to instruction is limited to before 9:00 a.m. and after 2:00 p.m. weekdays.
  - d. Be polite; do not send abusive, threatening, bullying, intimidating and/or harassing messages to others.
  - e. Use appropriate language.
  - f. Do not reveal personal addresses or phone numbers of students or colleagues.
  - g. Note that Electronic Mail (e-mail) is not guaranteed to be private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities must be reported to authorities. TPSS provides email accounts for its employees and does not warrant access to other email services or messaging services. Web mail is not permitted on any computers located in classrooms or used by students except for TPSS provided student accounts (currently Gaggle).
  - h. Hardware or software shall not be destroyed, modified, or abused in any way.
  - i. Do not use the network in a way that would disrupt the use of the network by other users (e.g. downloading huge files during prime time, sending mass E-mail messages, installation of unapproved software, or annoying other users using chat, talk, or write functions). The network should be used only for research, information gathering, and academic practice directly related to school assignments and extracurricular projects supervised by school faculty.
  - j. The network is NOT designed to be used as a radio or television for the classroom. Any such use should be DIRECTLY related to instruction. All streaming media not directly related to instruction is prohibited.

- k. Malicious use of the network to develop programs that harass other users or infiltrate a computer, computing system, or network is prohibited. Use of the network to damage the software components of a computer or computing system is prohibited.
  - l. E-mail, chat, and instant messaging of any form should be used for legitimate and responsible communication only. Hate mail, including statements that bully, threaten, intimidate and harass, discriminatory remarks, cursing, and other anti-social behaviors are prohibited on the network.
  - m. The illegal installation of copyrighted software for use on district computers is prohibited.
  - n. Use of the network to access or process pornographic materials, inappropriate text files, and files dangerous to any individual or group is prohibited.
  - o. Chat rooms may be used only with approval from building level administrator and the guidance of the teacher for instructional activities. A letter requesting the authorization to chat should be sent to the TPSS Technology Department.
  - p. Transmission of any materials in violations of any U.S. or state regulation is prohibited. This includes - but is not limited to - copyrighted software, music, videos, and other materials protected by trade institutions and ALL threatening or obscene material.
  - q. Use for product advertisement, political lobbying, or illegal activities is strictly prohibited.
  - r. Gaining unauthorized access to resources or entities is prohibited. Students should access only those files that belong to them or which they have been granted permission to use by faculty.
  - s. Files stored on district computers and servers should be limited to those relating to formal school courses or activities.
  - t. Invading the privacy of individuals is prohibited.
  - u. Using the account or password of another user is prohibited. Distribution of passwords by other than designated staff is forbidden.
  - v. Posting communications without the author's consent is prohibited.
  - w. Posting or sending anonymous messages is prohibited.
4. **Security** – Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the Internet or WAN, you must notify the school administrator who will notify the TPSS Technology Department. Do not demonstrate the problem to other users. Any user identified as a security risk or having a history of problems with other computer users may be denied access to technology resources.
  5. **Vandalism** – Vandalism will result in cancellation of privileges and/or other disciplinary actions. Vandalism related to technology is defined as any malicious attempt to harm or destroy the equipment or data of another user, LAN, WAN, or other networks that are connected to the TPSS network. This includes, but is not limited to, the uploading or creation of computer viruses.
  6. **Consequences of Misuse** – According to the Tangipahoa Parish School Board Policy Manual, school principals shall discipline any user who accesses, sends, receives, or configures electronically any profane, threatening, bullying, intimidating, harassing, pornographic and/or obscene language or pictures. Any individual failing to follow the above “Terms and Conditions” is subject to appropriate disciplinary measures as determined by school administrators and the TPSS Technology Department. Students may receive consequences of steps 2 through 6 on the assertive discipline ladder. Should a student utilize the internet, cameras, cell phones, “IPODS” and other technologies to communicate with students or staff using off campus resources that subsequently cause “material disruption” at school, he/she will be disciplined in accordance with the parish assertive discipline plan. Should cell phones be used for **any** purpose during the regular school day, except during an emergency situation, student will receive consequences of steps 2 through 6 on the assertive discipline ladder at the discretion of the administrator.
  7. **Bypassing Filters or Security Systems** - Attempts to remove, modify, or bypass software, hardware, and configurations installed to prevent Internet or other access to pornographic material, other objectionable materials, or prohibited resources is forbidden. Such violations shall result in cancellation of computer use privileges and mandatory suspension from school.
  8. **Monitoring** – Teachers agree to instruct the students on acceptable technology use and monitor all student technology use to insure student compliance with this policy. Students agree that teachers and administrators have the right to monitor ALL student activity using the network and other technology resources.

## **CODE OF CONDUCT**

This Code of Conduct applies to all users of these technology resources. Honesty, integrity, and respect for the rights of others should be evident at all times. Photographs may only be permitted with current, signed state department of education photo release on file. Students will not be identified by name in conjunction with a recognizable picture. Students will only be identified by first names.

The technology user is held responsible for his/her actions and activities. Unacceptable uses of the network will result in disciplinary action including possible revocation of these privileges.

**Directions:** After reading the Tangipahoa Parish School System Code of Conduct and Terms and Conditions, please read and fill out the appropriate portions of the following contract completely and legibly. Please return this contract to your teacher or school administrator.

### **USER (Student or Teacher) TECHNOLOGY CONTRACT**

I have read the Acceptable Use Policy. I understand and will abide by the regulations. I understand misuse is unethical and illegal. Should I commit any violation, my access privileges may be revoked and disciplinary action will be taken. A signed copy of this document must be on file with the teacher. In the case where the teacher is the user, a copy will be on file in the office.

User Name (please print): \_\_\_\_\_

User Signature: \_\_\_\_\_

Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

### **PARENT TECHNOLOGY CONTRACT**

As the parent or guardian of this student, I have read the Terms and Conditions of the Tangipahoa Parish School System Acceptable Use Policy. I understand that this access is designed for educational purposes and Tangipahoa Parish School System has taken available precautions to monitor student access. However, I also recognize it is impossible for Tangipahoa Parish School System to restrict all controversial materials, and I will not hold them (TPSS) responsible for the materials acquired on the network. I hereby give my permission for my child to have school use of technology including the Internet.

Parent or Guardian (please print): \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

Daytime Phone Number: \_\_\_\_\_

Evening Phone Number: \_\_\_\_\_

## **TECHNOLOGY GUIDELINES FOR PARENTS**

By taking responsibility for children's online computer use, parents minimize any potential risks of being online. Make it a family rule to:

- Never give out identifying information- home address, school name, or telephone number- in a public message such as chat rooms or bulletin boards. Be sure you are dealing with someone that both you and your child know and trust before giving personal information out via E-mail. Think carefully before revealing any personal information such as age, marital status, or financial information. Consider using a pseudonym or un-listing your child's name if your service allows it.
- Get to know the services your child uses. If you don't know how to log on, get your child to show you. Find out what types of information the service offers and whether there are ways for parents to block out objectionable material.
- Never allow a child to arrange a face-to-face meeting with another computer user unknown to you without your permission. If a meeting is arranged, make the first one in a public spot, and be sure to accompany your child.
- Never respond to message or bulletin board items that are suggestive, obscene, belligerent, threatening, or make you feel uncomfortable. Encourage your child to tell you if they encounter such messages. If you and/or your child receive a message that is harassing, of a sexual nature, or threatening, forward a copy of the message to your service provider and ask for assistance.
- If you become aware of the transmission, use, or viewing of child pornography while online, immediately report this information to your local law enforcement agency, the National Center for Missing and Exploited Children (1-800-843- 5678), and your local service provider.
- Remember that people online may not be who they seem. Because you can't see or hear the person, it would be easy to misrepresent himself or herself. Someone indicating that "she" is a "12-year-old girl" could in reality be a 40-year old man.
- Remember that not everything you read online is true. Sources should be checked and evaluated before the information is assumed to be true. Any offer that is too good to be true probably is. Be careful about offers that involve coming to a meeting or having someone visit your house.
- Set reasonable rules and guidelines for computer use by your children, including the amount of time they spend on the computer, time of day they access online services, and the areas of online services they visit. Parents should spend time "surfing" the Internet with their children and should monitor its use by children.
- Discuss these rules and post them near the computer as a reminder. Remember to monitor compliance with the rules, especially when it comes to the amount of time your children spend on the computer. Your child's excessive use of online services and bulletin boards, especially late at night, may be a clue there is a potential problem. Remember that personal computers and online services should not be used as babysitters.
- Make online explorations a family activity. Consider keeping the computer in a family room rather than in the child's bedroom. Get to know your child's online friends just as you get to know all of his/her other friends.
- There is software available and ISP-based services that attempt to filter undesirable information on the Internet. This software sets limits and defines restrictions. You can contact your online provider for more information as to what software is recommended for this purpose.