TECHNOLOGY ACCEPTABLE USE POLICY (AUP)

The Tangipahoa Parish School Board believes it is necessary for all persons to become aware of the acceptable use of technology. 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.

Age and grade appropriate classroom instruction shall be provided regarding Internet and cell phone safety. Such instruction shall include appropriate online behavior, interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response, as well as areas of concern as authorized in state and federal law.

In addition, the School Board, in conjunction with local law enforcement agencies, shall develop and distribute age and grade appropriate information to each student regarding Internet and cell phone safety and online content that is a threat to school safety. The information shall include the following:

- Instruction on how to detect potential threats to school safety exhibited online, including posting on any social media platform.

- Visual examples of possible threats.

- The process for reporting potential threats, which shall be in accordance with the procedures referenced in policy *EBBB, School and Student Safety.*

Such information shall be either distributed to or explained to students and school personnel at the beginning of each school year and shall be posted on an easily accessible page of the School Board's website and the website of each school.

If information reported to a school is deemed a potential threat to school safety, the school shall present the written form and any further evidence to local law enforcement.

Technology, particularly Internet access and email, is available to students and employees in the Tangipahoa Parish School System. The Tangipahoa Parish School Board's goal in providing these resources to its 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. All users, including students, employees, or any other users of School Board computers, hardware, and district network shall abide by all policies of the School Board and any applicable administrative regulations and procedures.

All users shall sign the *Technology Contract* on a yearly basis. The signature shall be binding and indicates that he/she has read the terms and conditions carefully, understands their significance, and shall adhere to their provisions. These should be kept on file at each school or office.

TERMS AND CONDITIONS

1. Acceptable Use - Technology resources in the Tangipahoa Parish School System (TPSS) shall ONLY be used to support teaching and learning.

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, the Tangipahoa Parish School System Director of Technology or the Superintendent or his/her designee.

3. Acquisition of Technology - ALL hardware and software purchases and installations shall be pre-approved by the TPSS Technology Department.

    A. All technology hardware and software resources purchased by TPSS are the property of the Tangipahoa Parish School Board and are loaned to students and faculty for their use.

4. Appropriate Network Usage - Users are expected to abide by the Tangipahoa Parish School System rules of network etiquette and Digital Citizenship as put forth by the TPSS Digital Citizenship curriculum. These include, but are not limited to the following:

    A. Be polite; do not send abusive, threatening, bullying, intimidating and/or harassing messages to others.

    B. Use appropriate language

    C. Hardware or software shall not be destroyed, modified, or abused in any way.

    D. 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.

E. 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.

F. 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.

G. Using the network for commercial purposes, gambling, financial gain, fraud, illegal acts, or threatening the safety of a person is prohibited.

H. Use of the network to access or process pornographic materials, inappropriate text files, and files dangerous to any individual or group is prohibited.

I. Network use for product advertisement, political lobbying, or illegal activities is strictly prohibited.

J. The posting or transmission of images or information in any format related to the school, staff, or students that are defamatory, abusive, pornographic, or which could be construed as threatening or impugning the character of another person is prohibited.

5. Security - Security on any computer system is a high priority, especially when the system involves many users. If a user can identify a security problem on the Internet or WAN, he/she 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.

A. Do not discuss or reveal personal addresses, phone numbers or any other personal identifiable information of students or colleagues.

B. Gaining unauthorized access to resources or entities is prohibited. Users should access only those files that belong to them or which they have been granted permission to use by faculty or coworkers.

C. Files stored on district computers and servers should be limited to those relating to formal school courses or activities.

D. Sharing logins and using the account or password of another user is prohibited. Distribution of passwords by other than designated staff is forbidden.

E. Users shall log off or lock their personal accounts when they step away from the computer for more than a few moments to prevent unauthorized access.

F. 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.

6. E-mail - Electronic Mail (e-mail) is not guaranteed to be private. The TPSS Superintendent and Technology Department personnel who operate the system have access to all mail. Messages relating to or in support of illegal activities must be reported to authorities.

A. TPSS provides email accounts for its employees and students and does not warrant access to other email services or messaging services. Tangischools e-mail accounts are to be used for professional correspondence.

B. Web mail is not permitted on any computers located in classrooms or used by students except for TPSS provided student accounts.

C. E-mail signatures shall ONLY include the following:

Name and Position; School or Office; Physical Address; Voice and Fax numbers; Email address and/or website address; School Mission Statement;

D. Users shall not post or forward e-mail chain letters" or send annoying or unnecessary messages to others.

E. Users shall not use district e-mail to mass email and "spam" any users (internal and external) with unauthorized communications or solicitations.

F. E-mail, chat, and instant messaging of any form should be used for legitimate and responsible communication only. Use of these technologies for commercial purposes, financial gain, fraud, illegal acts, or threatening the safety of a person is prohibited.

G. Hate mail, including statements that bully, threaten, intimidate and harass, discriminatory remarks, cursing, and other anti-social behaviors are prohibited on the network.

7. Use of Electronic Devices

A. The use of all recording devices of any kind, including but not limited to all kinds of cameras, video recorders, audio recorders, etc. except for instructional purposes or TPSS official business is strictly prohibited.

B. Student use of the Internet, cameras, cell phones, "IPODS" and/or any other electronic systems, on or off campus, that subsequently causes *substantial disruption* to the educational environment, interferes with the rights of others, or can be considered a threat, will result in the student receiving discipline in accordance with the parish assertive discipline plan.

8. Violating Copyright Laws

A. The illegal installation, downloading, copying or sharing of copyrighted software for use on district computers is prohibited.

B. 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.

9. 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. The student and his/her parents are responsible for compensating TPSS for any losses, costs or damages incurred by the School Board for violations of School Board policies/procedures and school rules while the student is using school computers, including the cost of investigating such violations.

10. Consequences of Misuse

A. 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.

B. The use of off campus resources including web pages, social networking sites, or Web tools that subsequently cause "material disruption" at school

is prohibited and the responsible student will be disciplined in accordance with the parish assertive discipline plan.

C. Any individual failing to follow the above provisions of this and other pertinent School Board provisions is subject to appropriate disciplinary measures as determined by school administrators and/or the Superintendent. Students may receive consequences of steps 2 through 6 on the assertive discipline ladder.

D. Employees who choose to violate the *Acceptable Use Policy* may be subject to adverse personnel action.

11. Monitoring - Teachers shall instruct the students on responsible technology use and monitor all student technology use to ensure 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.

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.

Revised: May 5, 1998
Revised: August, 1999
Revised: July 10, 2006
Revised: July 1, 2008
Revised: August, 2008
Revised: March 17, 2009
Revised: July 21, 2009
Revised: August 2, 2011
Revised: June 27, 2013
Revised: July 21, 2015
Revised: April 16, 2018
Revised: November 7, 2018
Revised: July 2019

Ref: 7 USC 254 (*Children's Internet Protection Act* (CIPA));La. Rev. Stat. Ann. ' §17:81, 17:100.7, 17:280, 17:410; Board minutes, 3-19-96, 5-5-98, 7-10-06, 7-1-08, 3-17-09, 7-21-09, 8-2-11, 6-27-13, 7-21-15, 4-16-18, 11-7-18.