Jarrell Independent School District Acceptable Use Policy

Jarrell Independent School District offers a wide area computer network with Internet access and email services for teachers, and staff within the school system. The network, and other school system technological resources provide opportunities to enhance instruction, appeal to different learning styles, and meet the educational goals of the board. Through the school system's technological resources, users can observe events as they occur around the world, interact with others on a variety of subjects, and acquire access to current and in-depth information. Access includes local, national, and international connections to (1) libraries, companies, agencies and businesses; (2) discussion groups on a variety of subjects; (3) information news services; and (4) electronic mail communication.

Acceptable uses of technological resources are limited to activities that support learning and teaching, except when otherwise specifically authorized by the superintendent in the best interest of the schools system. Use of technological resources should be integrated into the educational program. Technological resources should be used in teaching the TEA Curriculum Standards and in meeting the educational goals of the board. The Curriculum Committee should provide suggestions for using technological resources in the curriculum guides. Teachers are encouraged to further incorporate the use of technological resources into their lesson plans. The superintendent shall ensure that school system computers with Internet access comply with federal requirements regarding filtering software, Internet monitoring, and Internet safety policies. The superintendent shall develop any regulations and submit any certifications necessary to meet such requirements. In addition, the superintendent or designee shall develop any other rules, procedures, forms, or other guidance needed to implement this policy.

A. REQUIREMENTS FOR USE OF TECHNOLOGICAL RESOURCES

School system technological resources include, but are not limited to computers, interactive whiteboards and other electronic devices, networks, the Internet, phones, copiers, facsimile machines, televisions, and video-recorders. The use of school system technological resources is a privilege, not a right. Students are given the privilege to use the Internet along with the responsibility of using it properly. Before using school system computers or electronic devices or accessing the school network or Internet, students and employees must provide a signed agreement indicating that they understand and will strictly comply with the requirements of this policy and any other related rules or procedures established by the superintendent or designee. Students also must provide the signature of a parent or guardian.

Failure to adhere to the requirements of this policy will result in disciplinary action, which may include immediate revocation of user privileges. Willful misuses of any school system technological resources may result in disciplinary action and/or criminal prosecution under applicable state and federal law. All students and employees must receive a copy of this policy annually.

Students are expected to learn and follow the guidelines set forth in this policy and must provide a written statement, signed by the student and his or her parent/guardian, acknowledging that (1) they agree that the student will adhere to all requirements and guidelines in this policy, and (2) the student assumes responsibility for his or her own actions.

Employees should maintain the highest ethical behavior in using the Internet and should promote that behavior among students. When using technological resources in the classroom, instructional personnel shall:

1. make every attempt to maintain the curricular focus of Internet use by locating and directing students toward sites on the Internet that support that focus;
2. ensure that student users have written permission from the parent or guardian;
3. make reasonable efforts to supervise a student's use of the Internet during instructional time;
4. model and provide instruction in the ethical and appropriate use of the Internet in a proper school setting as provided in this policy.

B. DISTRICT PROVIDED DEVICES

When using district provided technology devices, users are accountable for the responsible use of the devices. Use of district provided devices is a privilege which may be revoked at any time. Violation of these policies will be subject to normal disciplinary action.

1. Content and Software – district equipment is to be used for educational purposes only. Music, videos, games and software must be district approved and installed.
2. Configuration – users may not alter the configuration of the device or install passwords on screensavers, BIOS settings menus, or deletion of files or folders. Deletion of some files may also result in a computer failure and may interfere in the ability to complete classwork, directly impacting grades.
3. Equipment Repairs – if the computer fails while in use, a decision will be made to determine if the failure was due to the equipment, or due to improper use. If the failure is due to improper use, the student or parent may be held liable for repairs.
4. Loss or Damage – if equipment is issued to the user and the property is damaged, lost, or stolen, the user is responsible for the cost of repair or replacement based upon the fair market value at the date of loss. Loss or theft of property must be reported to the District within one business day, and a police report must be filed within 48 hours of the occurrence if applicable.

a. If the equipment is stolen:
i. Notify the Principal or Supervisor immediately, or within one business day
Ii. File a police report within 48 hours of the occurrence

b. If the equipment is lost:
i. The user will be responsible to pay the school district the total costs associated with replacing the equipment.

c. If the equipment has been deliberately damaged or vandalized:
i. The user will be charged for the replacement or repair of the equipment.

C. GUIDELINES FOR ACCEPTABLE USE: ALL USERS

1. School system technological resources are provided for school-related authorized purposes only. Acceptable uses of such technological resources are limited to responsible, efficient, and legal activities that support learning and teaching. Use of school system technological resources for commercial gain or profit, or for amusement or entertainment is prohibited. School system technological resources shall not be used for charitable endeavors without prior approval of the superintendent.
2. Under no circumstance may software purchased by the school system be copied for personal use.
3. Students and employees must comply with all board policies, administrative regulations, and school standards and rules in using technological resources. All applicable laws, including those relating to copyrights and trademarks, confidential information, and public records, apply to technological resource use. Any use that violates state or federal law is strictly prohibited. All rules of the Code of Conduct apply to students' use of the Internet and other technological resources.
4. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally accessing, downloading, storing, printing or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages or other material that is obscene, defamatory, profane, pornographic, harassing, abusive or considered to be harmful to minors.
5. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).
6. Users must respect the privacy of others. When using e-mail, chat rooms, blogs or other forms of electronic communication, students must not reveal personally identifiable, private or confidential information, such as

the home address, telephone number, credit or checking account information, or social security number of themselves or fellow students. In addition, school employees must not disclose on the Internet or on school system websites or web pages any personally identifiable information concerning students (including names, addresses or pictures) without the written permission of a parent or guardian or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA) or policy 4700, Student Records. Users also may not forward or post personal communications without the author's prior consent.

7. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks and/or data of anyone connected to the server or the Internet. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance. Users must scan any downloaded files for viruses. Users may not attempt to repair or maintain technological resources unless expressly authorized or directed to do so by the technology director or designee.

8. Users may not create or introduce games, network communications programs, or any foreign program or software onto any school system computer, electronic device or network without the express permission of the technology director or designee.

9. Users are prohibited from engaging in unauthorized or unlawful activities, such as "hacking" or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems or accounts.

10. Users are prohibited from using another individual's computer account. Users may not read, alter, change, block, execute or delete files or communications belonging to another user without appropriate authorization or the owner's express prior permission. In addition, employees shall not share or reveal their passwords or user IDs for any data system. All employees with access to NCWISE or other sensitive data are responsible for safeguarding their user IDs and passwords.

11. If a user identifies a security problem on a technological resource, he or she must immediately notify the wide area network supervisor or other designated system administrator. Users must not demonstrate the problem to other users. Any user identified as a security risk will be denied access.

12. Views may be expressed as representing the view of the school system or part of the school system only with prior approval by the superintendent or designee.

D. INTERNET SAFETY

Before a student may use the Internet for any purpose, the student's parent must be made aware of the possibility that the student could obtain access to inappropriate material. The parent and student must sign a consent form acknowledging that the student user is responsible for appropriate use of the Internet and consenting to monitoring by school system personnel of the student's e-mail communication and use of the Internet. The board is aware that there is information on the Internet that is not related to the educational program. The board also is aware that the Internet may provide information and opportunities to communicate on subjects that are not suitable for school-age children and that many parents would find objectionable. School system personnel shall take reasonable precautions to prevent students from having access to inappropriate materials, such as violence, nudity, obscenity or graphic language that does not serve a legitimate pedagogical purpose. The superintendent shall ensure that the Internet service provider or technology personnel have installed a technology protection measure that blocks or filters Internet access to audio or visual depictions that are obscene, that are considered pornography or that are harmful to minors. School officials may disable such filters for an adult who uses a school-owned computer for bona fide research or another lawful educational purpose. School system personnel may not restrict Internet access to ideas, perspectives or viewpoints if the restriction is motivated solely by disapproval of the ideas involved.

E. PRIVACY

No right of privacy exists in the use of technological resources. Users should not assume that files or communications created or transmitted using school system technological resources or stored on servers or hard drives of individual computers will be private. School system administrators or individuals designated by the

superintendent may review files, monitor all communication, and intercept email messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School system personnel shall monitor online activities of individuals who access the Internet via a school-owned computer. Communications relating to or in support of illegal activities will be reported to the appropriate authorities. Information in electronic messages is not anonymous and is subject to disclosure to third parties under state and/or federal law in certain circumstances.

F. PERSONAL WEBSITES

No right of privacy exists in the use of technological resources. Users should not assume that files or communications created or transmitted using school system technological resources or stored on servers or hard drives of individual computers will be private. School system administrators or individuals designated by the superintendent may review files, monitor all communication, and intercept email messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School system personnel shall monitor online activities of individuals who access the Internet via a school-owned computer. Communications relating to or in support of illegal activities will be reported to the appropriate authorities. Information in electronic messages is not anonymous and is subject to disclosure to third parties under state and/or federal law in certain circumstances. The superintendent may use any means available to request the removal of personal websites that substantially disrupt the school environment or that utilize school system or individual school names, logos or trademarks without permission.

1. **Students** - Though school personnel generally do not monitor students' Internet activity conducted on non-school system computers during non-school hours, when the student's online behavior has a direct and immediate effect on school safety or maintaining order and discipline in the schools, the student may be disciplined in accordance with board policy. Please see the most recent version of the Student Code of Conduct documentation (located at www.jarrellisd.org under the 'Parent Resources' tab) for clarification.

2. **Employees** - Employees are to maintain an appropriate relationship with students at all times. Employees are encouraged to block students from viewing personal information on employee personal websites or online networking profiles in order to prevent the possibility that students could view materials that are not age-appropriate. If an employee creates and/or posts inappropriate content on a website or profile and it has a negative impact on the employee's ability to perform his or her job as it relates to working with students, the employee will be subject to discipline up to and including dismissal. This section applies to all employees, volunteers and student teachers working in the school system. The superintendent will establish guidelines regarding employee use of media and technology to communicate with students outside the classroom.

CONSEQUENCES FOR INAPPROPRIATE USE:
Noncompliance with applicable regulations will result in a) suspension of access to District technology resources; b) revocation of account; c) disciplinary action consistent with District policies and regulations. Violations of law may result in criminal prosecutions as well as disciplinary action by the District.

STUDENT INTERNET USE AGREEMENT

User's Full Name (please print):_____

Home Address:_____

Home Phone:_____

I understand and will abide by the Jarrell Independent School District Technology Acceptable Use Policy and understand that if I violate this policy my Internet access privileges may be revoked and school disciplinary and/or legal action may be taken against me. I further understand that any violation that constitutes a criminal offense will be reported to law enforcement authorities.

User Signature_____ Date: _____/_____/_____

PARENT or GUARDIAN *(If you are under the age of 18 a parent or guardian must also read and sign this agreement.)*
As the parent or guardian of this student, I have read the Jarrell Independent School District Technology Acceptable Use Policy. I understand that access to the Internet is designed for educational purposes only. I also recognize that it is impossible to restrict access to all inappropriate materials and I will not hold the school system responsible for materials acquired on the network. I accept full responsibility for my child's compliance with the Technology Acceptable Use Policy and hereby give my child permission to use the JISD network.

Parent or Guardian's Name (please print):_____

Signature: _____ Date: _____/_____/_____

Legal References: U.S. Const. amend. I; Children's Internet Protection Act, 47 U.S.C. 254(h)(5); Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; 17 U.S.C. 101 *et seq*.; 20 U.S.C. 6777; G.S. 115C-325(e), -391

STAFF INTERNET USE AGREEMENT

User's Full Name (please print):_____

I understand and will abide by the Jarrell Independent School District Technology Acceptable Use Policy and understand that if I violate this policy my Internet access privileges may be revoked and school disciplinary and/or legal action may be taken against me. I further understand that any violation that constitutes a criminal offense will be reported to law enforcement authorities.

User Signature_____ Date: ____/____/_____