



Jarrell Independent School District

Acceptable Use Policy

Jarrell Independent School District, herein referred to as the LEA(Local Education Agency), offers a wide area computer network with Internet access and email services for staff and students within the LEA. The network and other LEA 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 various subjects; (3) information news services; and (4) electronic mail.

Acceptable uses of technological resources are limited to activities that support learning and teaching, except when deemed necessary by the superintendent in the best interest of the LEA. The 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 board's educational goals. 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 the LEA's computers with Internet access comply with federal requirements regarding filtering software, Internet monitoring, and Internet safety policies. The superintendent shall develop regulations and submit 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.

REQUIREMENTS FOR USE OF TECHNOLOGICAL RESOURCES

The LEA's 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. Employees 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.

Failure to adhere to the requirements of this policy will result in disciplinary action, which may include immediate revocation of user privileges. Willful misuse of any school system's 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.

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.

DISTRICT PROVIDED DEVICES

Each employee is responsible for all instructional materials and technology equipment that is not returned in an acceptable condition by the employee. A fee may be charged if an employee fails to return technology equipment in an acceptable condition. Students who fail to return technology in an acceptable condition forfeit the right to a replacement technology equipment until all previously issued equipment is returned or reimbursed.

1. **Maintenance and Repair** - Normal and reasonable wear and tear are expected. Gross negligence will not be tolerated. It is the employee's responsibility to provide reasonable care and to coordinate required repairs through the principal's campus designee. are responsible for the cost of repair and replacement of damaged and lost devices. A loaner device will be distributed only when an employee's device is being repaired due to normal wear and tear.
2. **Device Chargers** – Employees are expected to bring their device to school fully charged and to bring their device charger. A replacement/loaner charger will not be available unless the employee brings their damaged charging device.
3. **Content and Software** – District equipment is to be used for educational purposes only. Music, videos, games, and software must be district-approved and installed.
4. **Configuration** – Users may not alter the configuration of the device or install passwords on screensavers, BIOS settings menus, or delete files or folders that JISD put on the device. Deletion of some files may also result in a computer failure and may interfere with the ability to complete and use applications needed.
5. **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 employee may be held liable for repairs.
6. **Stolen device-** In the event of a stolen device, the incident must be reported to campus officials within one business day of when the theft occurred. A police report will need to be submitted within 2 business days to the LEA's police department.

GUIDELINES FOR ACCEPTABLE USE: ALL USERS

1. The LEA's 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 circumstances 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 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.
8. 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.
9. 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 PIEMS or other sensitive data are responsible for safeguarding their user IDs and passwords and not saving the data on unsecured or unencrypted drives.
10. 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.

INTERNET SAFETY

Before an employee may use the Internet for any purpose, the employee must sign a consent form acknowledging that they are responsible for the appropriate use of the Internet and consenting to monitoring by school system personnel of their use of the Internet. The board is aware that there is information on the Internet that is not related to educational programs. School system personnel shall take reasonable precautions to prevent employees 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.

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 the online activities of individuals who access the Internet via a District-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.

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 the 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 the school system or individual school names, logos, or trademarks without permission. **Employees** - Employees are to always maintain an appropriate relationship with students. Employees are encouraged to block students from viewing personal information on employee personal websites or online networking profiles 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.



Jarrell Independent School District

504 N. 5th Street, Jarrell, TX 76537 - www.jarrellisd.org - (512) 746-2124

TECHNOLOGY AGREEMENT

Employee Name: _____ ID #: _____

Campus: JES DCES IES BCES JMS JRMS JHS District

CONSEQUENCES FOR INAPPROPRIATE USE:

Noncompliance with applicable regulations will result in A) suspension of access to District technology resources; B) revocation of account; and 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.

EMPLOYEE AGREEMENT:

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.

Employee Signature: _____

Date: ____/____/____