

Jonesboro Independent School District

Acceptable Use Policy as Approved by the School Board

Nondiscrimination Statement

Jonesboro ISD does not discriminate on the basis of race, religion, color, national origin, sex or disability in providing education services. The Principal has been designated to coordinate compliance with the nondiscrimination requirement of Title IX of the Education Amendments of 1972, as amended. The Principal has been designated to coordinate compliance with the nondiscrimination requirements, Section 504 of the Rehabilitation Act of 1973.

Jonesboro ISD does not discriminate on the basis of disability by denying access to the benefits of District services, programs or activities. To request information about applicability of Title II of the Americans with Disabilities Act (ADA), interested persons should contact the Principal.

Electronic Communication and Data Management

The Principal or District Technology Director shall implement, monitor and evaluate electronic media resources for instructional and administrative purposes.

Availability of Access

Access to the District's electronic communications system, including the Internet, shall be made available to students and employees exclusively for instructional and administrative purposes and in accordance with administrative regulations.

Access to the District's electronic communications system is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to comply with such regulations and guidelines. Noncompliance with applicable regulations may result in suspension or termination of privileges and other disciplinary action consistent with District policies [See DH, FN, FNC, FNCJ, FO and the Student Code of Conduct]. Violations of the law may result in criminal prosecution as well as disciplinary action by the district.

Acceptable Use

The Principal or District Technology Director shall develop and implement administrative regulations, guidelines and user agreements consistent with the purposes and mission of the District and with law and policy governing copyright [See EFE].

Monitored Use

Electronic mail transmissions and other use of the electronic communications system by students and employees shall not be considered confidential and may be monitored at any time by the Principal or District Technology Director to ensure appropriate use for educational or administrative purposes.

Disclaimer of Liability

The District shall not be liable for inappropriate use of electronic communication resources or violations of copyright restrictions, users' mistakes or negligence or costs incurred by users. The District shall not be responsible for ensuring the accuracy or usability of any information found on the Internet.

Local Regulations

Electronic Communication and Data Management

The District's system will be used only for administrative and educational purposes consistent with the District's mission and goals. Commercial use of the District's system is strictly prohibited.

The District will provide training to employees in the proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the District's system will emphasize the ethical use of this resource.

Copyrighted software or unauthorized software may not be placed on any computer connected to the District's network system at any time without permission from the holder of the copyright and Technology Director.

System Access

Access to the District's electronic communications system will be governed as follows:

1. With the approval of the Principal, District employees will be granted access to the District's system.
2. The District will require that all passwords be changed every year.
3. A teacher may apply for a class account and, in doing so, will ultimately be responsible for use of the account. Teachers with accounts will be required to maintain password confidentiality by not sharing passwords with students, other employees or non-employees.
4. Students completing required course work on the system will have first priority for use of District equipment after school hours.
5. Any system user identified as a security risk or having violated District and/or Campus computer use guidelines may be denied access to the District's system.

District Network Technology Directors Responsibilities

The Network Technology Director for the electronic communications system and the Principal will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system.
2. Be responsible for issuing and assignment of all computers, laptops, associated hardware and software.
3. Ensure that all users of the District's system complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the campus Principal's office and District Technology Director's Office.
4. Ensure that employees supervising students who use the District's system provide training emphasizing the appropriate use of this resource.
5. Ensure that the school district stays in compliance with Federal and State laws governing and regulating copyright laws and license agreements of all software use and utilization on the District's system.
6. Ensure that all software purchased or installed is compatible with the current district network system.
7. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure proper use of the system.
8. Be authorized to establish a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed to be inappropriate.
9. Set limits for disk utilization on the system as needed.
10. Establish all passwords and login hours.
11. Ensure that a student or students are supervised at all times while using any computer, including computers in all labs. This will be strictly enforced.

Individual User Responsibilities

The following standards will apply to all users of the District's electronic information/communications systems:

On-Line Conduct

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy.
3. System users may not use another person's system account without written permission from the Principal or District Technology Director.
4. System users must purge electronic mail in accordance with established retention guidelines.
5. System users may redistribute copyrighted programs or data only with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable Federal and State copyright laws, District policy and administrative regulations. Documents must be filed with District Technology Director's office.
6. System users may not upload public domain programs to the system. System users may not download public domain programs for their own use or non-commercially redistribute a public domain program.

The District will cooperate fully with local, state or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

Internet Safety Policy as Approved by the Jonesboro ISD School Board

Internet users are expected to use the Internet as an educational resource. The following procedures and guidelines are used to help ensure safe and appropriate use of the Internet at Jonesboro Independent School District.

Student Expectations in use of the Internet

- a. Students shall not access material that is obscene, pornographic, child pornography, "harmful to minors," or otherwise inappropriate for educational uses.
- b. Students shall not use school resources to engage in "hacking" or attempts to otherwise compromise system security.
- c. Students shall not engage in illegal activities on the Internet.
- d. Students shall not reveal their user password or use another user's password at any time. This is a direct violation of the school's policy and will be strictly enforced.
- e. Students shall not disclose personal information, such as name, school, address, and telephone number outside the school network.
- f. Students shall not download games, software, toolbars, music, screen savers, background images and/or pictures of any nature. This will be strictly enforced. Violation will result in disabling of the student's user account.
- g. Students shall not change any monitor or computer setting.
- h. Students shall not insert music CD's, "burned" or homemade CD's or a disk into computers at any time.
- i. Students may not insert **any** USB chips, SIM chips, DIM chips (memory chips) into computers at any time. Violation will result in disabling of student user account.

Any violation of school policy and rules may result in loss of school-provided access to the Internet. Additional disciplinary action may be determined in keeping with existing procedures and practices regarding inappropriate language or behavior. When and where applicable, law enforcement agencies may be involved.

Staff Expectations in Use of the Internet

- a. Staff shall not use or access material that is obscene or is child pornography or otherwise inappropriate for educational uses.
- b. Staff shall not share their user password or use another user's password at any time (family members, other staff members, etc). This is a direct violation of the school's policy and will be strictly enforced.
- c. Staff shall not use the school's resources to engage in "hacking" or any attempts to otherwise compromise system security.
- d. Staff shall use electronic mail and other forms of direct electronic communication for school-related purposes only.
- e. Staff shall not forward e-mails with pictures attached to them.
- f. No Student, family member or friend shall be allowed on a teacher's or staff member's computer at any time.
- g. Staff members shall not download games, software, toolbars, music, screensavers, background images and/or pictures of any nature. This will be strictly enforced. Violation will result in disabling of teacher's or staff member's user account.
- h. Video Systems shall be returned in the same condition as when they were checked out (all remotes and units clean). No student is allowed to use any of the remotes and must be at least five (5) feet from the unit while in use. (Exceptions: During a PowerPoint presentation they may stand beside the unit.) Students shall not touch the screen or change any settings.
- i. All USB chips, SIM chips, DIM chips (memory chips) or "burned" (homemade) CD's must be scanned in the Technology Server room before they may be used. Violation will result in disabling of the user's account.

Any violation of school policy may result in loss of school-provided access to the Internet. Additional disciplinary action may be determined in keeping with existing procedures and practices. When and where applicable, law enforcement agencies may be involved.

Enforcement of Policy

- a. Jonesboro Independent School District uses a technology protection measure that blocks or filters Internet access to some Internet sites that are not in accordance with the policy of Jonesboro Independent School District.
- b. A Jonesboro Independent School District staff member may override the technology protection measure that blocks or filters Internet access for a student to access a site with ***legitimate educational value*** that is wrongly blocked by the technology protection measure that blocks or filters Internet access upon **approval of the Principal and Technology Director**.
- c. Jonesboro Independent School District staff will monitor students' use of the Internet through direct supervision to ensure enforcement of the policy. At no time is a student allowed to use the school's computer without direct supervision.