

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT REGULATION

The Superintendent/designee will oversee the District's electronic communications system(s). The District will provide training in proper use of the system(s) and will provide all users with copies of acceptable use guidelines. All training in the use of the District's system(s) will emphasize the ethical use of this resource. The Jacksonville Independent School District provides technology resources to its students and staff for educational, administrative, and limited personal use. The goal in providing these resources is to promote educational excellence in the district by enabling resource sharing, innovation and communication with the support and supervision of parents, teachers and support staff. The use of technology resources is a privilege, not a right.

With access to computers and people all over the world comes the potential availability of material that may not be considered to be of educational value. Jacksonville ISD firmly believes the value of information, resource sharing, and research capabilities available outweigh the possibilities that users may obtain material that is objectionable and not consistent with the educational goals of the district.

Computers may be searched with reasonable suspicion of policy/regulation violations or subject to routine, random inspection for administrative purposes.

WHAT ARE DISTRICT TECHNOLOGY RESOURCES?

The District's computer systems and networks are any configuration of hardware and software. The systems and networks include all of the computer hardware, operating system software, application software, stored text and data files. This includes electronic mail, local databases, externally accessed databases (such as the Internet), CDROM, DVD, optical media, clip art, digital images, digitized information, telecommunications devices, and all new technologies as they become available. The District reserves the right to monitor all technology resource activity.

CONSENT REQUIREMENTS

No original work created by any District student or employee will be posted on a web page under the District's control unless the District has received written consent from the student (and the student's parent) or employee who created the work. No personally identifiable information about a District student will be posted on a web page under the District's control unless the District has received written consent from the student's parent. An exception may be made for "directory information" as allowed by the Family Education Records Privacy Act and District policy.

SYSTEM ACCESS

Access to the District's electronic communication system(s) will be governed as follows:

1. District employees will be granted access to the District's system(s) after signing the acceptable use agreement for electronic communications or with approval of immediate supervisor.
2. Students in grades PK–12 will be granted access to the District's system(s) by their teachers, as appropriate. Students in grades K-12 will be assigned individual accounts under the direct supervision of a specific teacher and with the permission of the District's Director of Technology.
3. Elementary teachers will be assigned a class account and will be ultimately responsible for use of the account.
4. Any system user identified as a security risk or as having violated the District and/or campus computer use guidelines may be denied access to the District's system(s).

CAMPUS LEVEL RESPONSIBILITIES

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system(s).
2. Ensure that employees and students complete and sign an agreement form to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the campus administrator's or supervisor's office.
3. Ensure that employees supervising students who use the District's system(s) provide training emphasizing the appropriate use of this resource.
4. Ensure that proper procedures are followed in requesting and acquiring all new hardware or software.

INDIVIDUAL USER RESPONSIBILITIES

The following standards will apply to all users of the District's electronic information/communication system(s):

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.

2. The system(s) may not be used for illegal purposes, in support of illegal activities or for any other activity prohibited by District policy or regulations.
3. System users shall not attempt to log on or log on to a computer or email system by using another's password. Assisting others in violating this rule by sharing information or passwords is unacceptable.
4. System users may not distribute personal information about themselves or others by means of the electronic communication system(s).
5. System users may not redistribute copyrighted programs or data except with the written permission of the copyright holder/designee. Such permission must be specified in the document or must be obtained directly from the copyright holder/designee in accordance with applicable copyright laws, District policy and administrative regulations.
6. System users shall not download any program file, executable program or java applet without prior approval from the District Technology Director or designee. You shall not load any application, game, operating system, applet, graphic, sound or video file onto any computer system without prior approval from the District Technology Director or designee.
7. System users shall not bring floppy disks, CD-ROMS, memory sticks and other storage media to use on any computer system without receiving approval from the District Technology Director or designee.
8. System users may not submit or publish messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation or illegal.
9. System users may not purposefully access materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation or illegal.
10. System users should be mindful that use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.
11. System users shall not waste District resources related to the electronic communication system(s).
12. System users shall not gain access to information resources, email, files and documents of another user without permission.
13. System users shall not use the network for financial gain, political or commercial activity.
14. Political use to advocate for or against a candidate, office holder, political party, or position is prohibited.
15. System users shall not attempt to harm equipment, materials or data.
16. System users will be responsible for the care and maintenance of their systems. Maintenance issues should be submitted in a work order.

USER SECURITY RESPONSIBILITIES

1. Your username and password should be protected from unauthorized use at all time. Do not post any of this information where others can view it.
2. Do not share your password via email at any time.
3. Ctrl+Alt+Del on your keyboard to lock your computer screen anytime you are away from your computer.

ELECTRONIC MAIL and INSTANT MESSENGER

1. The District's software and hardware that provide email and instant messenger capabilities are funded with public monies. For that reason, it should not be considered a private, personal form of communication.
2. Email and instant messages are recorded and stored and may be requested under the Public Information Act.
3. Email will be monitored.
4. Tampering with electronic mail of other users is prohibited.
5. Forgery of electronic mail messages or transmission of unsolicited junk email or chain messages is prohibited.
6. Attachments sent via email have been limited to 20 megabytes. You may find some PowerPoint presentations, videos, photographs, or graphic files will be too large to email.
7. Remember, deleted files can be recovered.
8. System users are asked to maintain electronic mail or outdated files on a regular basis. Email shall be checked on a daily basis.

VANDALISM PROHIBITED

Any malicious attempt to harm or destroy District equipment or data of another user of the District's system(s), or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses. System users shall not attempt to gain unauthorized access to the district-wide area network or to any other computer system(s) through the district-wide area network or go beyond your authorized access. This includes attempting to log in through another person's account or access another person's files.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate consequences.

FORGERY PROHIBITED

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy or modify the electronic mail of other system users, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person's user ID and/or password is prohibited.

INFORMATION CONTENT/THIRD-PARTY SUPPLIED INFORMATION

System users and parents of students with access to the District's system(s) should be aware that use of the system(s) may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material. It is possible that you may access some material you might find objectionable. While the District has a technology protection measure in place, it is not possible to absolutely prevent such access. A system user who gains access to such material is expected to discontinue the access as quickly as possible and report the incident to the supervising teacher or Campus Administrator.

A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's system(s) and will be subject to disciplinary action in accordance with the Student Code of Conduct. An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies.

NETWORK ETIQUETTE

System users are expected to observe the following network etiquette:

1. Be polite. Messages typed in capital letters are the computer equivalent of shouting and are considered rude.
2. Use appropriate language. Swearing, vulgarity, ethnic or racial slurs and any other inflammatory language are prohibited.
3. Pretending to be someone else when sending/receiving messages is prohibited.
4. Transmitting obscene messages or pictures is prohibited.
5. Using the network in such a way that would disrupt the use of the network by other users is prohibited.
6. Users shall not send chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.

PRIVACY EXPECTATION

System users have no privacy expectation in the contents of their personal files on any District computer system. Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating the Acceptable Use Policy or the law. An individual search will be conducted if there is reasonable suspicion that a user has violated the law or the established Acceptable Use Policy. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.

District employees should be aware that their personal files are discoverable under the statutes of the state of Texas.

TERMINATION REVOCATION OF SYSTEM USER ACCOUNT

Termination of an employee's or student's access for violation of District policies, regulations or applicable laws will be effective on the date the campus administrator or District Technology Director receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

DISCLAIMER

The District's system(s) is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system(s) and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system(s) will meet the system user's requirements, or that the system(s) will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services and all other information expressed by system users, information providers, service providers or other third-party individuals in the system(s) are those of the providers and not the District.

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