Administrative Procedures

Judson Independent School District

C - Business and Support Services No. 2		C2
Page 1 of 8	Attachment(s):	
August 20, 2018		

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

The Judson Independent School District provides technology resources to its students, staff, contractors, consultants, visitors, parents, and community for educational and administrative purposes. The goal in providing these resources is to promote educational excellence in the District's schools by facilitating resource sharing, innovation and communication with the support and supervision of parents, teachers and staff.

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 in the context of the school setting. Judson ISD firmly believes that the value of information, interaction, and research capabilities available outweighs the possibility that users may obtain material that is not consistent with the educational goals of the District.

Thus, the purpose of this procedure is to ensure that computer assets are used only by authorized persons for authorized purposes, that computer related hardware, software and data are protected from mischief and that accountability is established for achievement of these objectives. All employees, students, parents, volunteers, vendors and other users are obligated to know and follow the procedures outlined for the appropriate use of electronic communication and data management.

Proper behavior, as it relates to the use of computers, is no different than proper behavior in all other aspects of Judson ISD activities. All users are expected to use the computers and networks in a responsible, ethical, and polite manner. This procedure is intended to clarify those expectations as they apply to computer and network usage and District Policy.

DEFINITION OF DISTRICT TECHNOLOGY RESOURCES

The District's computer systems and networks are any configuration of hardware, software, and/or network resources. The systems and networks include all of the servers, switches, 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), CD-ROM, optical media, clip art, digital images, digitized information, communications technologies, blogs, wikis, SMS, instant messaging, unified communications, web sites, digital documents and new technologies as they become available. The District reserves the right to monitor all technology resource activity and take appropriate actions when violations are observed.

DEFINITION OF ACCEPTABLE USE

Use of information technology resources can be broadly categorized as acceptable or prohibited:

- Acceptable use of information technology resources is legal use consistent with the mission of the Judson ISD, i.e., use that furthers the District's mission of teaching and learning.
- Prohibited use is illegal use and all other use that is not acceptable.

CONDUCT ON THE SYSTEM

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

1. The system user in whose name a system account is issued will be responsible at all times for its proper use. Passwords and other information related to system and network access are restricted to that individual and must never be shared.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or procedures.
3. System users may not disable, bypass, or attempt to disable or bypass a filtering device on the District's electronic communications system.
4. Communications may not be encrypted so as to avoid security review or monitoring by system administrators.
5. System users may not gain or seek to gain unauthorized access to resources or information.
6. System users may not use or attempt to use the network and/or it's resources for financial gain, political or commercial activity.
7. System users may not access, submit, transmit, publish, or display materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
8. System users may not redistribute copyrighted programs or data except 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 copyright laws, District policy, and Administrative Procedures.
9. System users may not waste District electronic communication system resources (e.g. email spamming, running servers, running file sharing software, etc.). **(Please refer to C12)**
10. In order to maintain an accurate inventory, computer systems may not be moved from one room to another except by the Desktop Services department. System users must submit a move request via the Help Desk. **(Please refer to C9)**
11. System users may not connect non-District technology equipment to the wired network without written consent of the Chief Technology Officer. **(Please refer to CS)**
12. Only Technology Services evaluated and approved technology and software may be purchased and used on the electronic communications system. **(Please refer to C10 and C11)**

SECURITY

Networks need to be set up with multiple levels of access. It is the responsibility of the Technology Services Department or designee to issue and maintain application security rights to the school employees and review these security rights on a regular basis. The access level to the application is determined by the immediate supervisor and/or system administrator and is based on the need to access data or resources.

Security violations should be reported immediately to the Technology Services Department. Failure to report these types of security concerns is a violation of District policy. **(Please refer to CQ Local & Legal)**

Campus/Department Level Responsibilities

Immediate Supervisors or designee is responsible for:

1. Disseminating, collecting signed permission forms, and enforcing the District Acceptable Use Guidelines for the District's system at the campus level, and
2. Ensuring that employees supervising students who use the District's systems provide information to students emphasizing the appropriate and ethical use of this resource.
3. Monitoring use of technology resources in their department/campus.

Individual Level Responsibilities

The following standards will apply to all users of the District's computer network systems:

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

2. System users are asked to delete electronic mail or outdated files on a regular basis following document retention guidelines as instructed by the Judson ISD Records Retention Officer.
3. System users will be responsible for the care and operation of their systems. Computer or software issues should be reported to the Help Desk.
4. System users will be responsible for following all copyright laws.
5. Securing all computers, mobile devices, teaching tools and removable media.
6. System users shall screen lock computers when they are to be left unattended.

Other Prohibited Uses That Are Security Violations

1. Causing a security breach to District, computers, electronics, or other network resources.
2. Using port scanning, non-approved remote access technologies, phishing, network floods, DNS attacks, SQL injection, IP spoofing, sniffers, honey pots, or similar technologies on the District network.
3. Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, malware, spyware, adware, and/or key loggers.

SYSTEM ACCESS

1. Prior to gaining access, system users are required to sign an agreement form **(C2-A Employee Agreement for Acceptable Use of Electronic Communications System and C2-E Member of Public Agreement for Acceptable Use of Electronic Communications System, JISD Student Handbook Acknowledgement Form)** acknowledging they have read and agree to abide by all District policy and regulations regarding District technology resources.
2. With approval from the immediate supervisor and the system administrator, District employees will be granted access to specific data sources and resources consistent with their job function and roles.
3. Password security and confidentiality are the sole responsibility of the user. At no time will the Technology Services Department or any designee of the Technology Services Department request a system user reveal his or her password.
4. The system user in whose name a system account is issued will be responsible at all times for its proper use. Passwords and other information related to system and network access are restricted to that individual and must never be shared with anyone else.
5. Whenever possible, passwords to District resources must meet complexity requirements. Please see **Password Security Guidelines** below, for more information.
6. Any system user identified as a security risk or having violated District Acceptable Use Guidelines may be denied access to the District's system. Other consequences may also be assigned.

PASSWORD SECURITY GUIDELINES

1. Employee passwords must meet the following minimum complexity requirements where possible.
    a. Be at least eight (8) characters in length and contain at least 3 of the following 4 types of characters:
        i. Lower case letters (e.g. a-z)
        ii. Upper case letters (e.g. A-Z)
        iii. Numbers (e.g. 0-9)
        iv. Special characters (e.g. !@#$%"&*()_+1--=\'{}[]:";'<>?,./)
    b. Minimum password age of 3 days and a maximum password age of 90 days.
    c. Unique to two iterations of password history. The system will record password history and not allow the last two passwords to be reused.
    d. Cannot contain significant portion of
        i. The user's name, birth date or employee IDs.
        ii. Words found in a dictionary, whether spelled forwards or backwards, or a word preceded or followed by a digit
        iii. Words that are slang, dialect, jargon, etc.
        iv. Common keyboard sequences, such as "qwerty89.. or ..abc123..
2. Passwords should not be written down. If it must be written down, try to write it in a way that cannot be deciphered (such as using a hint) and store it securely in a safe, unlikely-to-be discovered location (e.g. not under the keyboard or on the monitor).
3. Information on how to change passwords should be provided with the password. If it is not, contact the person or office issuing the password for instructions.

4. Do not let applications, browser, or key chains remember passwords that provide access to sensitive systems or data.
5. If you think your password may have been compromised, notify Technology Services and your supervisor immediately.

CONFIDENTIAL INFORMATION AND PROTECTION OF DATA

Users must ensure that District proprietary, confidential, and sensitive information remains within the control of the District at all times, and is not disclosed to parties that are not authorized to access the information. Conducting District business that results in the storage of District proprietary, confidential or sensitive information on personal or non-District controlled environments, including devices maintained by a third party with whom the District does not have a contractual or other business agreement, is prohibited. **District Board policies FL (Legal) and FL (local) define confidential and sensitive student information and stipulates how such information must be managed and maintained. (Please refer to C3)**

PHYSICAL ASSET PROTECTION

A user is responsible for ensuring the safety, security of District electronic assets/equipment under his or her control. District electronic assets and equipment, including laptop/notebook computers, tablets, cell phones, pagers, PDA's, cameras, MP3 players, projectors, and document cameras must be appropriately secured and supervised during the workday. During non-working hours, staff must take reasonable and appropriate steps to secure District electronic assets and equipment, including, but not limited to, locking rooms, closets, storage areas, cabinets, drawers, carts, etc. in which the asset and/or equipment resides. Items left at the District overnight must be appropriately secured and placed in a locked drawer, cabinet, cart, or office. If laptops or other devices must be placed in a vehicle, employee shall ensure that they are placed out of sight, in the trunk of a vehicle, prior to departure for destination. Any theft of any District electronic assets/equipment must be reported to the Judson ISD Police Department, local law enforcement agency, and the Technology Services Department immediately. Prior to leaving employment with the District, a user must ensure that all equipment under the user's control has been checked in by his or her supervisor. A user may be required to pay for replacement equipment in the case of loss or damage resulting from negligence related to the care or security of equipment or failure to adhere to policies or regulations regarding technology.

ELECTRONIC MAIL AND INSTANT MESSAGING

Email is one of the most used communication tools in both our constituents' homes and their work places. It is also an integral part of all District classrooms and offices. As such, the following must be adhered to for all email and instant messaging type communications:

1. All electronic communication is governed by the Electronic Communication and Data Management procedures C-2.
2. The software and hardware that provides us email capabilities has been publicly funded. For that reason, it should not be considered a private, personal form of communication.
3. Remember to think before you write and before you push the "send" button. Do not put anything in email that you do not want to see on the front page of the local paper. Consider making a call, or having a face-to-face conversation with the person you are emailing. Remember that you do not have to respond to an individual via email just because they contacted you that way. The District has the right to monitor all email use and will be storing copies of all emails. Always keep in mind that you, the user, are ultimately responsible for your email content and conduct.
4. Limited use of Judson ISD email for personal communication is permitted, as long as it does not interfere with an employee's ability to perform their duties nor interfere with their work. This communication should not be considered private and is governed by Electronic Communication and Data Management procedures.
5. System users may not send, forward, or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
6. During student contact time in the classroom, staff members should not use email, instant messenger programs or SMS.
7. Staff members should set aside time to check and respond to email messages at least once per day.
8. Judson ISD has established email distribution groups for the easy and convenience of employees. All campus employees must gain the approval of their campus principal to disseminate information through the distribution groups. Campus employees are allowed to email only those groups associated with their campus. District-level

distribution groups require authorized access that can be obtained by filling out ***Form C2-B: Request for Exchange Distribution Group Access***.

9. Requests for confidential personal information on students or staff members should not be honored via email. It is critical for a personal contact to be made with any individual requesting confidential personal information. This relates particularly to any requests for student grades, discipline, attendance, employee addresses, social security numbers, health data or related information. At no time should confidential information ever be sent to a non-Judson ISD email address, without being encrypted by Technology Services.
10. Security information such as passwords should not be sent via email for any reason.
11. Emails sent with the intent of advertising or selling any item, product or service (whether personal or for a business) would be considered commercial and are not permitted.
12. Since email access is provided for school business related use, please do not forward messages that have no educational or professional value. An example would be any number of messages that show a cute text pattern or follow a "chain letter" concept.
13. Subscriptions to an Internet listserv should be limited to professional digests.
14. System users should be mindful that use of school-related electronic mail addresses and fax transmissions might cause some recipients or other readers of that communication to assume they represent the District or school, whether or not that was the user's intention.
15. System users should avoid actions that are likely to increase the risk of introducing viruses to the system, such as opening email messages from unknown senders and loading data from unprotected computers.
16. Please notify your immediate supervisor if you receive email of a threatening nature. The Technology Services Department will attempt to track down the source of that email and prevent you from receiving any additional unsolicited mail.

Supervisors can request access to employee email AND/OR files by filling out ***Form C2-C: Request for Access to Employee Electronic Data***. Access will be granted if:

1. The employee is no longer employed by Judson ISD. ; or
2. Investigation of inappropriate activity is approved by a director in the Human Resources Department.

By Fall 2011, supervisors will automatically be given access to a former employee's email and files, and will no longer need to fill out C2-C.

EMAIL RETENTION PROCEDURES

1. Purpose

The following email retention procedures are intended to help Judson ISD employees understand how Judson ISD email will be retained and what their role is. The information covered in these procedures includes information that is either stored or shared via electronic mail. All users should familiarize themselves with the email retention background and procedures below.

2. Background

According to Texas State Records Management rules, as established by the Texas State Library and Archives Commission, there is no specific retention period for email, because it is not a record in itself but merely a means of transmitting information. This is true of any document, whether digital or paper. The content of the document must be looked at to determine if and how long it should be retained. Retention periods are determined by the content, nature, and purpose of records, and are set based on their legal, fiscal, administrative, and historical values, regardless of the format in which they reside. The retention of any particular electronic mail message should be the same as the retention for records in any other format that document the same program function or activity. The procedures and training for retaining records at Judson ISD should be followed per the guidelines and training provided by the Records Retention Officer in the Department of Student Services.

Due to the transitory nature of email messages and the tremendous volume of messages, a print and retain approach at Judson ISD will consume a lot of staff time and printing resources. Additionally, while it would be ideal to file copies of email messages according to content either in paper format or electronically, the volume of email is overwhelming and likelihood of being able to enforce user compliance is low. Additionally email is further confused as to who needs to retain any particular message - the originator, the recipient, or the last person to reply? All of this would create an undue burden on Judson ISD staffs time.

3. Retention Procedures

Judson ISD starting no later than July 1, 2009, the District will begin a "retain all" approach to any employee email sent or received. All employee email will be archived on an appliance dedicated to the task. Email will be retained on the appliance hard drive for a period of at least 3 years for all Judson ISD staff. Additionally, all email will be stored on unalterable tape for a period of 7 years, covering most retention rules established by the Texas State Library and Archives Commission. Tapes will be stored off-site in a secure vault for restorations and/or investigatory purposes. If retention requirements dictate that a message needs to be retained beyond 7 years, the user must print and file the message. Tapes will be destroyed at the end of the retention period. Requests for emails for investigatory and Public Information Act appeals will be done according to normal processes. Requests to pull emails from long term tape backup will only be honored in extraordinary circumstances, as it can place an undue burden on IT staff. (Student email will only be retained for investigative purposes for limited time periods of about ninety days or when archival storage is full.)

USE OF NETWORK FILE SHARES

Judson ISD provides network file shares for the convenience of access and collaboration with peers. Users have the following responsibilities when utilizing these resources:

1. All use of file shares is subject to Electronic Communication and Data Management procedures C-2.
2. All files saved to a user's home drive or campus/department share must follow copyright and fair use guidelines as outlined below.
3. No personal files (MP3s, digital photos, movies, etc.) should be saved to the file shares or home directories.

Supervisors can request access to employee home directories by filling out ***Form C2-C: Request for Access to Employee Electronic Data***. Access will be granted if:

1. The employee is no longer employed as Judson ISD. ; or
2. Investigation of inappropriate activity is approved by a director in the Human Resources Department.

Generally, supervisors will automatically are given access to a former employee's email and files, and do not need to fill out C2-C.

COPYRIGHT

It is the policy of the Judson ISD that all employees, volunteers, and students are to abide by the federal copyright laws. Employees, volunteers, and students may copy both print and non-print materials as allowed by:

1. Copyright laws
2. Fair use guidelines
3. Specific licenses or contractual agreements
4. If permission is given in writing from copyright holder.

Employees, volunteers, and students who willfully disregard copyright laws are in violation of this policy, doing so at their own risk and assuming all liability.

FILTERING

The Chief Technology Officer will appoint a designee to select, implement, and maintain appropriate technology for filtering Internet sites containing material considered inappropriate or harmful to minors. All Internet access will be filtered for minors and adults on computers with Internet access provided by the school District.

The categories of material considered inappropriate and to which access will be blocked will include, but not be limited to: nudity/pornography; images or descriptions of sexual acts; promotion of violence; illegal use of weapons, drug use, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g., bomb making); unapproved online forums, unapproved instant messaging; non-instructional games and on-line gambling.

It is a violation of Judson ISD policy to disable, bypass, or attempt to disable or bypass a filtering device on the District's electronic communications system. Network Services recognizes that due to the nature of some issues (disciplinary or discovery) some users need special access within the filtering system. The content filtering system has various levels of access and are assigned based on a user's job function and need for access. A user can request relaxed or unfiltered access to the Internet by filling out ***Form C2-D: Request for Unfiltered Internet Access***, and gaining approval from their supervisor. All requests will be reviewed for necessity by the Director of Network Services.

MONITORING OF DISTRICT TECHNOLOGY RESOURCES

Electronic mail transmissions, other electronic communication and use of computer systems by students and employees shall not be considered private. Monitoring can occur while engaging in routine maintenance, carrying out internal investigations, preparing responses to requests for public records, administering systems, or disclosing messages, data, or files to law enforcement authorities. Monitoring can occur at any time to ensure appropriate use. The District reserves the right to monitor access to and use of email, instant messaging, the Internet, or other network or computer-related activity.

While, the District respects the contents of your files and email and does not regularly review all files or all email content as a part of normal daily activities, system administrators may become aware of file and/or email content while administering systems or using monitoring tools. Usage logs are frequently kept to diagnose problems and monitoring tools are used to ensure appropriate network use. Furthermore, the District will comply with the lawful orders of courts, such as subpoenas and search warrants. This compliance has included providing, when required, copies of documents/messages on District operated servers, computers, etc.

The District does not regularly review all electronic communication for the purpose of determining whether impermissible activity is occurring unless requested by campus or District administration. If a supervisor wishes to request access to an employee's electronic data, they must fill out ***Form C2-C: Request for Access to Employee Electronic Data***, and gain approval of Human Resources Department. However, in the course of administering the network and monitoring the network for violations of the Acceptable Use Agreement, system administrators may become aware of activity that poses a risk to the network's proper operation, risk to the security of data, risk to the District's reputation, risk to student well-being, and/or threatening to individual's safety. In such cases, Network Services staff may need to follow up with found issues by employee's supervisors, the Human Resources Department or campus administrators to ensure that corrective action is taken. Also, during the process of monitoring the network, any information obtained that indicates possible unauthorized distribution and/or procurement of copyrighted materials may be referred to Human Resources for further investigation.

VANDALISM PROHIBITED

Any attempt to harm, deface or destroy District equipment or materials, data on District's system, or any of the agencies or other networks to which the District has access is prohibited. Intentional attempts to degrade or disrupt system performance may be viewed as violations of District policy and regulations and, possibly, as criminal activity under applicable state and federal laws, including the **Texas Penal Code, Computer Crimes, Chapter 33**. Vandalism as defined above will result in the cancellation of system use privileges and possible prosecution. The party will be responsible for restitution of costs associated with cleanup, system restoration, hardware, or software costs.

SUSPENSION/REVOCATION OF SYSTEM ACCOUNTS

The District will suspend or revoke a system user's access to the Districts system upon violation of District policy and/or Administrative Procedures regarding acceptable use. Termination of an employee's account or of a student's access will be effective on the date the principal or campus coordinator receives notice of user withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

CONSEQUENCES OF IMPROPER USE

Improper, negligent, or unethical use may result in disciplinary actions consistent with the existing District policy, the Texas Penal Code, Computer Crimes, Chapter 33, or other applicable state and federal laws. This may also require restitution for costs associated with cleanup, system restoration, hardware, or software costs.

DISCLAIMER

The District's system 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 fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District uses a variety of vendor-supplied hardware, networks, and software. Therefore, the District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the user's requirements. Neither does the District warrant that the system will be uninterrupted or error-free, nor 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 are those of the providers and not necessarily the District's.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's computer systems and networks.

SECURITY POLICY FOR REVTRAK SYSTEM USERS

- Do not allow PANs (Primary Account Number- the 16-digit number printed on the front of a credit/debit card) to be distributed via unencrypted messaging technologies (e.g. e-mail, Instant Messenger, etc.)
- All cardholder hardcopy data should be destroyed once it is no longer needed. This should only be necessary in the case of a mailed order. Note that the best practice for a phone order is to enter it directly into the ***RevTrak*** Web Store and not to write the payment card information on paper.
    - The hardcopy materials should be destroyed (e.g. shredded, incinerated, pulped, etc.) such that reconstruction is not practically possible.

Attachments:

Form C2-A:	***Employee Agreement for Acceptable Use of Electronic Communications System***
Form C2-B:	***Request for Exchange Distribution Group Access***
Form C2-C:	***Request for Access to Employee Electronic Data***
Form C2-D:	***Change Internet Access Request***
Form C2-E:	***Member of Public Agreement for Acceptable Use of Electronic Communications System***

See these *INDEX* references for related procedures: Data Management and Security; District and Personal Cell Phone Use

Resources: **CQ (LOCAL) and CQ (LEGAL); Texas Penal Code, Computer Crimes, Chapter 33,JISD Student Handbook and Acknowledgement Form.**

Questions regarding this procedure should be addressed to Technology Services at 210-945-5580; 8205 Palisades Drive, San Antonio, Texas 78233

Approved.

Jose A Cortinas
Chief Technology Officer

Date: 8/27/2018

Jean M Bell
Superintendent

Date: 8/27/2018