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

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 softv 0 0 1 G[( )] 4MC 6(1 0 0 s(or)TJETBT1 0 0 1 69.

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:	***Request for Unfiltered Internet Access***
	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.

Date: 8-27-2018
Chief Technology Officer

Date: 8/27/2018