CROWLEY ISD ADMINISTRATIVE REGULATION

Board Policy: CQ(Local)

Date Effective: July 1, 2005
Date Revised: July 26, 2013

Re: Electronic Communication and Data Management

Introduction

The Crowley Independent School District provides technology resources to its students and staff 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. All users are expected to use the computers and computer networks in a responsible, ethical, and polite manner. This document is intended to clarify those expectations as they apply to computer and network usage and is consistent with District Policy.

The Director of Information and Technology Resources or designee will oversee the District's electronic communications system.

Definition of District Technology Resources

The District's computer systems, mobile devices, 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, optical media, clip art, digital images, digitized information, communications technologies, and new technologies as they become available. The District reserves the right to monitor all technology resource activity.

Acceptable Use

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

- Acceptable use of information technology resources is legal use consistent with the mission of the Crowley ISD, i.e., use that furthers the district's mission of learning and teaching.
- Allowable use is legal use for other purposes that do not impinge on acceptable use. The amount of Allowable use will vary over time based on the capacity reserve of information technology resources available beyond acceptable use.
- Prohibited use is illegal use and all other use that is neither acceptable nor allowable.

System Access

- Prior to gaining access, system users are required to sign an agreement form that they have read and agree to abide by all district policy and regulations regarding district technology resources.
- 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.
- Password security and confidentiality are the sole responsibility of the user. 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.
- 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.
- All mobile systems must have a managed solution (MDM) attached to the device in order to gain network access.

Security

The purpose of the Crowley ISD Administrative Regulation for Electronic Communication and Data Management 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 are obligated to know and follow the Crowley ISD Administrative Regulation for Electronic Communication and Data Management.

Networks need to be set up with multiple levels of access. It is the responsibility of the Technology Department to issue and maintain application security access to school employees. 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 Department. Failure to report such violations is a violation of district policy.

Campus/Department Level Responsibilities

Immediate Supervisors or designee are responsible for:

- Disseminating, collecting signed permission forms, and enforcing the District Acceptable Use. Guidelines for the District's system at the campus level, and
- Ensuring that employees supervising students who use the District's systems provide information to students emphasizing the appropriate and ethical use of this resource.

Individual Level Responsibilities

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

- System users in whose name a system account is issued will be responsible at all times for its proper use.
- System users are asked to delete electronic mail or outdated files on a regular basis.
- System users will be responsible for the care and maintenance of their systems. Maintenance issues should be reported to the Technology Department through the district online work request system, or by phone when a network services are down.
- System users are responsible for making backup copies of all important files as needed.
- System users will be responsible for following all copyright laws.

Conduct on the System

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

- 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.
- The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.
- System users may not disable, bypass, or attempt to disable or bypass a filtering device on the District's electronic communications system.
- Communications may not be encrypted so as to avoid security review or monitoring by system administrators.
- System users may not gain or seek to gain unauthorized access to resources or information. System users may not use or attempt to use the network and/or its resources for financial gain, political or commercial activity.
- System users may not access, submit, publish, or display materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
- 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 regulations.
- System users may not waste District electronic communication system resources (e.g. email spamming, distribution of videos or photos, listening to web radio, etc.).
- In order to maintain an accurate inventory, computer systems and telephones may not be moved from one room to another except by the Technology Department and with the approval of the immediate supervisor or principal. System users must submit a request via the technology work order system.
- System users may not connect non-District technology equipment to the network without written consent of the Technology Director.
- Only District evaluated and approved technology may be purchased and used on the electronic communications system.

Electronic Mail

Email has become one of the most used communications tools in both our constituents' homes and their work places. Email is an integral part of all Crowley Independent School district classroom and offices, the following points are important and must be followed:

- All electronic communication is governed by the Electronic Communication and Data Management. All terms that are covered in the Electronic Communication and Data Management (CQLegal, CQLocal), including user responsibilities and consequences for policy violations, apply to Email.
- The software and hardware that provides the District email capabilities has been publicly funded. For that reason, it should not be considered a private, personal form of communication. The contents of any communication of this type are governed by the Electronic Communication and Data Management (CQLegal, CQLocal).
- 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.
- Email accounts will be limited to 200 Megabytes of server storage space. Approval for additional storage must be requested by email and approved by the Executive Director of School Operations. Users will be responsible for backing up their email and removing it from the server.

- Staff members should set aside time to check and respond to email messages at least once per day.
- Requests for 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 personal information. This relates particularly to any requests for student grades, discipline, attendance or related information. In addition, security information such as username or password should not be sent via email for any reason.
- 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.
- 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.
- Subscriptions to an Internet listserv should be limited to professional digests due to the amount of email traffic generated by general subscriptions. Use a personal Internet email account to receive listserv subscriptions of a general nature.
- 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.
- 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.
- Please notify your immediate supervisor if you receive email of a threatening nature. The Technology Department will attempt to track down the source of that email and prevent you from receiving any additional unsolicited mail.

Copyright

It is the policy of the Crowley ISD that all employees, volunteers, and students are to abide by the federal copyright laws.

Employees, volunteers, and students may copy print or non-print materials allowed by:

1. Copyright laws
2. Fair use guidelines
3. Specific licenses or contractual agreements
4. Other types if permission is given in writing

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 Superintendent 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 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) ; non-educational games and online gambling.

System users may not disable, bypass, or attempt to disable or bypass a filtering device on the District's electronic communications system.

Computer Software

Our goal is to promote the use of appropriate, innovative software whenever possible. These guidelines will insure that the required support and installation process is in place before funds are expended. The current configuration on district computers does not allow unauthorized software installation. Unauthorized software installation may affect network and machine performance adversely and is prohibited by the policy and administrative regulations of Crowley Independent School District Technology Resources.

- All software must successfully complete a software approval process prior to purchase and installation. All installations will be done by a Crowley ISD technician, approved vendor or designee.
- Software will be installed only when there is documentation showing that the software purchase has gone through the process referenced above and that proper licensing has been purchased.
- Software purchased by staff using personal funds will be subject to all district policies and administrative regulations. Prior to purchase and install, the personal software must go through the district software approval process. All installations will be done by a Crowley ISD technician, approved vendor or designee. It is the Technology Department's strong recommendation that employees receive approval prior to purchase. If the software is not approved, it will not be installed, and the employee will forfeit the cost of the purchase.

Computer Hardware

- Absolutely no one except approved vendors, district technicians, and designee are authorized to install computer hardware on any district site.
- Campus computer systems may not be modified, upgraded, or replaced with donated equipment without the prior approval of the Technology Department.
- In order to maintain an accurate inventory, computer systems may not be moved from one room to another except by the Technology Department and with the approval of the immediate supervisor or principal. System users must submit a request via the technology work order system.

Acceptance of Technology Donations

All potential donations are to be evaluated by the Technology Department. Donations will be evaluated based on the ability to meet the following criteria:

- Supportive to the technology plan of the District.
- Meet or exceed current equipment level for compatibility and are compatible with the current and planned platforms at the school.
- Create no unanticipated or excessive financial burden for the district (construction, wiring, additional equipment, staffing, etc.)
- Require limited maintenance.
- Carry no unreasonable restrictions by the donor. Become the property of Crowley ISD.
- The Director of Information and Technology Resources will complete the Intent to Accept form or to request a monetary gift. (See Exhibit A)

Monitoring of District Technology Resources

Electronic mail transmissions and other use of the electronic communications system 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, 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.

The district respects the contents of your files and email and does not review file or email content as a part of normal daily activities. However, system administrators may become aware of file and/or email content while dealing with some system problems. Usage logs are frequently kept to diagnose such problems. Furthermore, the district will comply with the lawful orders of courts, such as subpoenas and search warrants. This compliance includes providing, when required, copies of discussions on district operated mailing list servers, files, instant messaging, etc.

The district does not review electronic communication for the purpose of determining whether impermissible activity is occurring unless requested by campus or district administration. However, in the course of assuring the viability of the district's network, system administrators may become aware of activity that poses a risk to the network's proper operation. In such cases, staff may need to disable or block access to ports involved in traffic levels deemed to pose a risk to the network's optimal functioning. Also, during the process of diagnosing potential problems to the network's proper functioning, any information obtained that indicates possible unauthorized distribution and/or procurement of copyrighted materials may be referred to the Human Resources Department for further investigation.

Vandalism Prohibited

Any attempt to harm, deface or destroy District equipment or materials, data on District's systems, 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 District's system upon violation of District policy and/or administrative regulations 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, regulations, 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.

The Technology Director will continue to regularly monitor the use of computers by employees in the district. If through this regular monitoring process, he/she discovers that viewing of pornographic websites have been attempted either through an employee's log in or actually on their computer, the following steps will be taken:

1. The first report will result in the employee receiving a letter from the Technology Director and the Technology Director will contact the employee's supervisor. The supervisor will conduct a conference with the employee and provide written documentation of the conference and the corrective action taken.

2. The second report shall be handled at the Central Office level and shall result in appropriate employee disciplinary action as defined in the Crowley ISD Employee Handbook.

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 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.

Exhibits:

Exhibit A – Intent to Accept or to Request a Monetary Gift

Exhibit A

Great Expectations Great Rewards

CISD

CROWLEY INDEPENDENT SCHOOL DISTRICT

Intent to Accept or to Request a Monetary Gift

District policy requires that all grants and gifts be reported. Based on size, various approvals or procedures are required.

Please complete this form for all unbudgeted monetary gifts requested or received, either solicited or unsolicited.

Who is the donor? (Contact name and information)

What is the amount of the gift?

_____

What is the date the funds were received?

_____

What school(s) or department(s) will benefit from the funds?

(Please attach documentation)

What are the reporting requirements, if any?

What will the funds be used for?

- ☐ Instruction
- ☐ Reading
- ☐ Math
- ☐ Science
- ☐ Social Studies
- ☐ English Language Arts
- ☐ Other:

Do you need assistance from the Finance Department?

☐ Yes ☐ No

If so, who should we contact?

Would you like the Communications Department to contact you upon award of the gift?

☐ Yes ☐ No

If so, who should we contact _____

Please print, sign and return this to:

Finance Department
512 Peach Street
Crowley, Texas 76036
817-297-5800
Fax: 817-297-5203

_____
Principal/Principal Designee

_____
Campus

_____

Chief of School Operations | Executive Director of Business Services | Superintendent Designee