Student/Community Internet/Network Safety Policy
For Du Quoin Community Unit School District #300

Introduction

It is the policy of Du Quoin Community Unit School District #300 to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activities; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification of minors; (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)]. Use of the Du Quoin Community Unit School District #300 Internet and computer access is a privilege, not a right. The school district reserves the right to remove access from individual users if there is abuse (see inappropriate network usage section for rules).

Definitions

Key terms are as defined in the Children's Internet Protection Act. *

Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the Du Quoin Community Unit School District online computer network when using either the Districts' networks or the Internet. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes the uses of any of the District computer networks listed below. These inappropriate uses are prohibited and may result in discipline or other consequences in accordance with the school/student/faculty handbook, board policy, or other administrative guidelines. Not following this policy may result in the loss of computer and Internet usage. Anyone vandalizing District property will be responsible for the cost of replacement. The network and its systems shall not be used to:

- Engage in activities which are not related to District educational purposes or which are contrary to the instructions from supervising District employees as to the network's use. Internet may only be used for school-related activities. Students and community members may not use Internet unless supervised by District personnel.
- Access, retrieve, or view obscene, profane or indecent materials. "Indecent materials" are those materials which, in context, depict or describe sexual activities or organs in terms patently offensive, as measured by contemporary community standards. "Obscene materials" are those materials which, taken as a whole, appeal to the prurient interest in sex, which portray sexual conduct in a patently offensive way in which, taken as a whole, do not have any serious literary, artistic, political or scientific value.
- Access, retrieve, view or disseminate any material in violation of any federal or state laws or regulations or District policy or rules. This includes, but is not limited to, improper use of copyrighted material; improper use of the System to commit fraud or with the intent to commit fraud; improper use of passwords or access codes; or disclosing the full name, home address, or phone number of any student, District employee, or System user.
- Check students' personal email accounts using school computers.

- Enter into chat rooms or access personal web pages or blogs (i.e. facebook, twitter or similar websites).
- Use or install any instant messaging software on the school computers.
- Transfer any software to or from the network without authorization from the Network Administrators.
- Engage in for-profit or non-school sponsored commercial activities, including advertising or sales, or purchase of goods or services online.
- Harass, threaten, intimidate, or demean an individual or group of individuals because of sex, color, race, religion, disability, national origin or sexual orientation. Never use the Internet to harm people in any way.
- Disrupt the educational process, including use that is reasonably foreseeable to result in a disruption, or interfere with the rights of others at any time, either during school days or after school hours.
- Disrupt or interfere with the network.
- Gain unauthorized access to or vandalize the data or files of another user, or bypass any security measures installed on computers or the network.
- Gain unauthorized access to or vandalize the network or the computer network of any other individual or organization.
- Forge or improperly alter electronic mail messages, use an account owned by another user, or disclose the user's individual password or that of another user.
- Invade the privacy of any individual, including violating federal or state laws regarding limitations on the disclosure of student/employee records. Do not give out unauthorized personal information over the internet.
- Download, copy, print or otherwise store or possess any data which violates federal or state copyright laws or these guidelines.
- Send nuisance electronic mail or other online messages such as chain letters, pyramid schemes, or obscene, harassing or other unwelcome messages.
- Conceal or misrepresent the user's identity while using the system.
- Post material on the District's web site without the authorization of the appropriate District administrator.
- Promoting, supporting or celebrating religion or religious institutions.
- Deploying student pictures with name tags on district and or school websites.
- Install or remove any software or hardware.
- Copy, distribute, or alter in any way software installed on District computers.
- Copy or use in any way someone else's work. Do not read, copy, delete, or change files that do not belong to you.
- Share or use someone else's password to log into or "hack" into school computers or networks.
- Use a machine designated only for teacher use for student use.

In addition to these rules above, there will be no installing equipment to our network without approval of the technology support person in each building. This includes but is not limited to: personal computers, wireless access points, hand held personal data organizers, and cell phones.

Email Archiving and Storage Policy

I. COVERAGE

This Policy Guidance is intended to cover all duquoinschools.org email account holders including board

members, employees and students. This guidance is issued as a "notice" to all duquoinschools.org email account users in regards to archiving of email.

II. BACKGROUND

In order to better manage the messaging system's large volume of email messages, tasks, and events; reduce the amount of required server storage space, as well as school and office workstation storage space used by email; reduce maintenance and installation times of school and office workstations, and enhance each school administrator's email search and recovery capabilities of their school's official email communications, Du Quoin School District #300 has implemented an automated email archiving plan.

This email archiving system reduces storage space and costs, while simplifying school administration and maintenance of the schools' messaging systems. Archiving tasks are now managed automatically and allow for seamless storage and retrieval of official archived information.

III. POLICY

The following policy applies to the District Mail Delivery System:

a.) This policy authorizes the implementation of an automated email archiving system, which automatically archives email events older than 30 days, and automatically purges all email older than 30 days from the district's mail server(s).

b.) Archived email will be maintained, off server, in a legally compliant, unalterable format, for a period of fifteen years, after which time it will be permanently destroyed.

c.) A mail administrator will conduct random monthly recovery tests of the email archiving system, to ensure that email is recoverable in the event of an official e-discovery request.

d.) In the event of a legal e-discovery request, or in the event that a school district can reasonably anticipate that a legal dispute may arise, all email communication relevant to the request or event will be retained until said request has been satisfied to parties involved.

e.) The district will assist email users in providing training to school personnel in methods and activities to ensure compliance with school district archival policies.

The following guidance applies to official office and school email usage and related policies:

In addition to the previously listed policy, the district would also like to remind users that they should follow the district's Inappropriate Network Usage Policy, Student Email Use Policy and Acceptable Use Policy (AUP) including the following guidelines:

a.) All school and office employees will be reminded that any email communication involving official school business should be conducted through the school's email system, and further, that the school's email system is for official school business usage only.

b.) All Du Quoin school email users are reminded that any reasonable expectation of privacy or confidentiality MUST include an understanding of the requirement to be compliant with all state and federal laws, as well as any relevant individual school district policies.

c.) Email messages are to be purged from workstations on a monthly basis. (This can be conducted through an automated policy on the school's network, or through individualized training of staff/faculty.)

d.) Any email messages that might be considered relevant to a student's permanent record, school purchasing matters, or school personnel matters, should be printed, and a copy kept on file at the school.

e.) In the event of a legal e-discovery request, or in the event that a school district can reasonably anticipate that a legal dispute may arise, all email communication relevant to the request or event will be retained until said request has been satisfied to parties involved.

This notice should also serve as a reminder to all email users and school personnel that Du Quoin School District #300 will comply with all applicable laws including the Illinois the State Records Act (5 ILCS 160/1 et seq.), the Illinois Local Records Act (50 ILCS 205/1 et seq.), the Illinois School Student Records Act (105 ILCS 10/1 et seq.), and the Illinois Freedom of Information Act ((5 ILCS 140/1 et. seq.), and any other applicable laws, regulations or rules.

References:

Illinois State Records Act (5 ILCS 160/1 et seq.)
Illinois Local Records Act (50 ILCS 205/1 et seq.)
http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=699&ChapAct=50%26nbsp%3BILCS%26nbsp%3B205%2F&ChapterID=11&ChapterName=LOCAL+GOVERNMENT&ActName=Local+Records+Act%2E
http://www.ilga.gov/commission/jcar/admincode/044/04404000sections.html.
http://www.iasb.com/pdf/nb0207.pdf
"Developments in School Law"
http://www.eschoolnews.com/news/top-news/index.cfm?i=42051
eSchool News Online – "Ruling: Schools Must Archive eMail" December 8, 2006
http://www.iasb.com/journal/j111208_05.cfm
Federal Rules of Civil Procedure (F.R.C.P.)
Amendments enacted December, 2006 (Rule 26, Rule 34)

Student Email Use Policy

- All student Electronic Mail (email) accounts are property of the Du Quoin Community Unit School District #300. Email activities must comply with the district's Student Email Use Policy, Inappropriate Network Usage Policy, Email Archiving and Storage Policy and all other applicable district, board, state and federal policies. The user accepts all responsibility to understand the policy.
- The student will be removed from the system after graduation, leaving the school district, or infractions outlined below.
- The primary purpose of the student electronic mail system is for students to communicate with school staff, approved outside resources related school assignments, and fellow students to collaborate on school activities. Account user names and passwords will be provided to appropriate district staff so they can monitor the account. Use of the district's email system is a privilege.
- Use of the email system will align with the school's code of conduct and the code will be used for discipline purposes. Communication through the district's email system will exhibit common sense and

civility. It will abide by the community's mode of acceptable behavior. Students are responsible for messages sent from their accounts. Students should not share their passwords.

- Messages posted on the district's email system cannot cause disruption to the school environment or normal and acceptable school operations. Only pre-approved, occasional and reasonable personal use of the district's email is permitted, providing that this does not interfere with the performance of the electronic mail system or disrupt the operation of the schools. Electronic mail from the system can be checked from home or from school computers, as long as it does not disrupt the operation of the classroom or school.
- The email system cannot be used to operate a personal business. The account may not be sold or otherwise reassigned. The account may be revoked if used inappropriately.
- Students will report any unusual activities such as "spam" communications, obscene email, attempts by adults to lure them into dangerous behaviors, and the like to the school's technology contact for action. Students should not forward chain letters, jokes, or graphics files.
- Students will not identify their home telephone numbers, or home addresses in any email correspondence.
- Electronic mail sent or received by the system is not confidential. Although the district does not make a practice of monitoring electronic mail, the administration reserves the right to retrieve the contents of user mailboxes for legitimate reasons, such as to find lost messages, to conduct internal investigations, to comply with investigations of wrongful acts or to recover from system failure.
- System administrators may create filters to scan for and eliminate viruses and large graphic files that are unrelated to the school district's operation.
- When issues arise, the district will deal directly with the student, school administration and/or parents/guardians. Improper use of the system will result in discipline and possible revocation of the student email account. Illegal activities on the system will be referred to law enforcement authorities for appropriate legal action.
- As it deems necessary, the district may contract with outside agencies to operate the student electronic mail system. If this arrangement is made, all parts of this statement remain in force.
- The district is responsible to ensure the efficient use of the electronic mail system. The interpretation of appropriate use and future revisions of this guideline are the responsibility of the district.
- If necessary, the district, at its discretion, may close the accounts at any time. Any updates or changes to this electronic mail agreement by the Board of Education or administration will be in effect.

Supervision and Monitoring

It shall be the responsibility of all members of the Du Quoin Community Unit School District #300 staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Technology Support Staff and the District Administration. Students and community members may not use the Internet unless supervised by District personnel.

CIPA definition of terms:

TECHNOLOGY PROTECTION MEASURE. The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

1. **OBSCENE**, as that term is defined in section 1460 of title 18, United States Code;
2. **CHILD PORNOGRAPHY**, as that term is defined in section 2256 of title 18, United States Code; or
3. Harmful to minors

HARMFUL TO MINORS. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion.
2. Depicts, describes, or represents, in a patiently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

SEXUAL ACT; SEXUAL CONTACT. The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.