Collinsville Community Unit School District No. 10

Technology Department

General Guidelines and Procedures For Staff Access to Electronic Resources

2013-2014

Table of Contents

Collinsville Community Unit School District No. 10
Technology Department

General Guidelines for Network Access, Internet Access and Email

2013-2014

Employees of Collinsville Community Unit School District No. 10 receive network accounts if needed that provide data storage space, access to the Internet, access to educational and personal productivity software as well as an email account. Use of the District's electronic networks is for EDUCATIONAL purposes. Use is a privilege, not a right of employment. Access to the District's network may be suspended or revoked following violations of the *Acceptable Use Policy.*

By law, all electronic communications using District equipment may be monitored by District administration. Monitoring equipment for email, chat, instant messaging, and Internet access is installed and records usage of all employees and students. Any staff member or student in violation of the District's AUP policy and any state or federal law will be subject to disciplinary and/or legal action.

Procedures for Requesting Network Access

In order to receive access to the District's electronic network, employees must accept a copy of the District's *Acceptable Use Policy* that describes appropriate use of District network resources (copy at end of this brochure).

The employee must also sign a copy of the *Acceptable Use Policy – Staff Acknowledgement Form* and return the form to the District's Technology Office for processing.
Both the *Acceptable Use Policy* and the *Staff Acknowledgement Form* documents can be obtained in any of the follow manners:

1. Requesting the documents from a Technology Department staff member at the building level.
2. Contacting the District's Technology Department at 618-346-6350, ext. 243
3. Accessing and printing the documents from the District's website:

www.kahoks.org
Employees link
Forms link
Technology link
Acceptable Use Policy – Staff (PDF Library)
Acceptable Use Policy – Staff Acknowledgement Form (PDF Library)

Data Storage and Server Account

Upon completion of the above documents and approval, the employee will have a network account created and a network username and password assigned along with e-mail access. The employee must change their password on their initial login. If any assistance is needed the employee should contact their building Technology Department staff member. Your password will need to be periodically changed (every 365 days) for security purposes.

The District uses Novell Netware/OES Linux as its network operating environment. Each employee is provided a username and allowed to select their own password. The user created password must conform to the district password policy. As outlined in the *Acceptable Use Policy* and by Board of Education Policy (CUSD Policy 6:235), the username and password may not be published or released to other individuals. **This information must be kept confidential**. If compromised, the password should be immediately changed by the employee. Assistance from a Technology Department staff member will be given if needed.

Employees SHOULD NOT save data or documents to any District computer's hard drive as such data is not secure and may be deleted at anytime. All data should be stored on the employee's server drive (designated by the drive letter H), USB key drive or other secure device, including "cloud services" if available). Documents and data stored to a computer's hard drive are NOT SECURE from other users and may be compromised.

Data stored in employee server accounts (H drives) is backed up on a regular basis. The District cannot recover any data **NOT** stored to the employee's server account.

Accessing Server Data from another District Location

Each building is part of the District's electronic wide area network (WAN). Buildings are electronically connected via leased fiber optic cable lines. A staff member's server account is maintained on the "home" school network. For example, a middle school math teacher's server account (H) is stored on the Collinsville Middle School server. An elementary band director's server account (H) is stored on the school server that is considered his/her "home" school such as Renfro Elementary School.

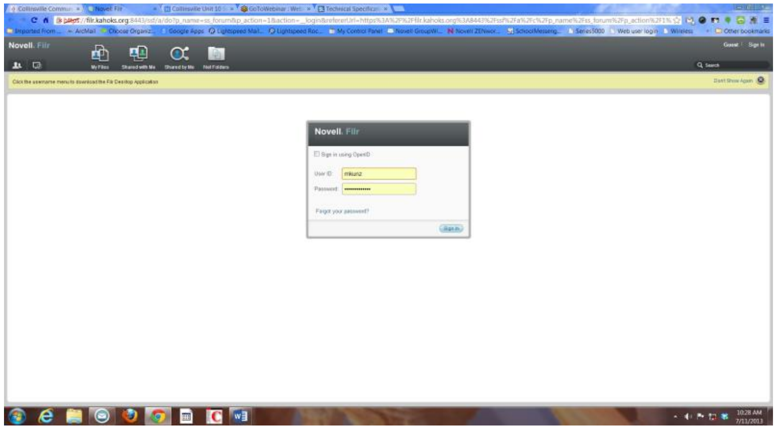
Employees have server accounts only at their home school. However, remote log-in is possible for all district staff members. In this process, the employee "logs" into their home school server from any District computer that is attached to a District local area network (LAN).

Employees do NOT have to do anything different to access their home directory contents as a process call "contextless login" is in place to find your user name and password.

Accessing Server Data from Remote Location

Employees may access data stored in their school network account from an outside location following the steps provided below. An employee's success at accessing and downloading files stored on the district server is dependent on the speed of the Internet connection from outside the district. Broadband connections such as via cable or DSL prove the most successful.

1. Navigate to www.kahoks.org
2. Click on **Departments**
3. Click on **Technology**
4. Click on **General Information**
5. Click on the **"Access Your District Files Here"** link
6. If a warning displays about a security issue please click continue
7. Enter your username and password
8. Click the sign in button and you will see the information shown below.



□ Sign in using OpenID

User ID: mkunz

Password: ••••••••••••••

Forgot your password?

Please contact a technology staff member for additional assistance if you have any questions. Further training will be provided as needed.

Unforeseen programming issues or network maintenance may prevent access to your server directory from time to time. The district cannot guarantee access to your network account at all times. If you are facing a deadline, please use a backup method of transporting your file(s) home or offsite such as a USB flash drive, Google Drive or MyBigCampus.

Email Account

The District uses Novell's Groupwise program for email accounts. Upon completion of the above documents, the employee may have an email account created depending on their position. This information will be provided to the employee by a Technology Department staff member. The email password will be the same as the staff member's Novell network password.

Record your email address, for future reference here:

_______________________@kahoks.org

The District's email system contains software to help limit the amount of SPAM received in an employee's email account; however, it is impossible to block all SPAM through the system. In addition, virus scanning software also attempts to remove the vast majority of infected attachments to email and halt the spread of viruses throughout the District's networks. Again, it is impossible to remove 100% of email virus attachments as virus code becomes more complex and difficult to detect and remove. To help limit the spread of computer viruses, Trojans and worms, an employee should NEVER open any email attachment if he/she does not know exactly what the attachment contains. Regardless of the employee's knowledge of the email sender, attachments may contain viruses. When in doubt about the validity of an email attachment, contact the sender before opening the file.

Email that is received and opened on a staff member's office or classroom computer continues to reside on the physical email server for the district (housed at Collinsville High School) until deleted by the user. To protect all emails and to store them for any needs at a later time, the District has instituted a program called ArcMail. The ArcMail backup program will store **ALL** email (even deleted) for a period of up to 1 year from the date it was created or received. The user does not have to do anything for the archive process to take place. It is the users responsibility to empty their email sent and trash items. Failure to do so will cause the users mailbox to become full and unusable until deleted items are removed.

To access the ArcMail program:

1. Navigate to www.kahoks.org
2. Click on **Employees link**
3. Click on **Email Access link**
4. Click on **Access Email archive system**
5. If a warning displays about a security issue please click continue
6. Enter you username and password. Please contact a technology staff member for additional assistance if you have any questions.

By law, all email sent and received through District electronic equipment, including files deleted from a user's account but not erased from the server, is public property and may be monitored or read by school officials.

Web Access to Email Account

The District provides Internet access to District email accounts called Novell Groupwise WebAccess.

To access the email account via the Internet:

1. Navigate to www.kahoks.org
2. **Employees link**

3. **Access District email link**
   (Resource Links)
4. Enter your username and password

Requesting Publishing of Email Address on District Web Site

Employees may elect to have their school email address published on the *Staff Directory* on the District's website. Employees should complete the *Download Permission to Post Email Address on CUSD#10 Web Site* form and forward it to the building Technology Department staff member for processing. The form may be accessed and printed from the District's website:

1. Navigate to www.kahoks.org
2. Click on **Employees**
3. Click on **Forms**
4. Click on **Technology**
5. Click on **Email**
6. Click on **"Employee request to have District Email address posted onCUSD10 Website."**

Once the signed form is received in the District's Technology office, the email address will be posted on the District's web site.

Internet Access and Internet Filtering

Once an employee has been provided with a network account, he/she has privileges for accessing the Internet from District computers. The District utilizes filtering software to meet the guidelines of the federal *Children's Internet Protection Act*. This federal legislation is designed to minimize access to pornography and other unacceptable Internet sites by minors. No filtering software can protect staff and students from all unwanted Internet sites due to the volume of new sites created and posted daily on the World Wide Web.

To meet the CIPA legislation, the District subscribes to a filtering service. This service automatically updates "NOT ALLOWED" sites on a daily basis. The District has the ability to manually block additional sites or allow blocked sites through the filter if they are deemed educationally acceptable by District standards. To limit the spread of viruses and to limit the influx of illegal file swapping and sharing, the District prohibits the downloading of certain files and services. Occasionally, these limitations prohibit staff members from accessing legitimate educational content. Staff members may request access to blocked sites on their own through the Lightspeed system with an explanation of the blocked site and rationale for why the site should be allowed. The filtering system used by the District does distinguish rights to sites by "user level" such as staff versus students. If a site is blocked for students, it may not be blocked for staff. Other sites that interfere with the educational purpose of the District, such as eBay, have been blocked on the wide area network. Monitoring software records traffic to inappropriate sites by USER NAME, time and sites visited. Violations of the *Acceptable Use Policy* are immediately reported to administration and may result in disciplinary action.

To access the staff request to unblock a website follow these steps:

Navigate to www.kahoks.org

1. Departments **link**
2. Technology **link**
3. Click on General Information
4. Find the link under Media Library titled "Staff Request/Blocked Website – (PDF)
5. Download the PDF file

We will attempt to review and acknowledge the request a.s.a.p. It is **HIGHLY** recommended to be sure to preview any website for access well ahead of any needs for educational access.

Students must be monitored by District personnel **at all times** while they are accessing the Internet or using electronic devices. Teachers **are highly encouraged** to research appropriate web sites for their students and limit the amount of unguided Internet searches conducted by students, particularly at the elementary grade levels. Proper instruction for Internet research must be provided by the classroom teacher.

Copyright

All District employees and students are expected to follow copyright law. Documents, text, graphical images and other content located on the Internet, unless noted by the web site author, are COPYRIGHTED. Material used for educational purposes from the Internet should be scrutinized for accuracy. Material used for resource purposes by staff and students should be cited to provide credit to the originator/author. District teachers and administrators should help students understand how to process the extensive amount of information available electronically. Staff and students must avoid plagiarism and copyright infringement by limiting any copying/pasting directly from the Internet and by providing proper documentation/citation of sites referenced.

Staff Web Pages

District teachers wishing to initiate, or create a classroom web page are encouraged to use an on-line web site such as Google Sites. Technology Department staff members can help get you started.

District Equipment Checkout

Any district staff member assigned a portable technology resource (such as a laptop computer, iPad, digital camera, portable printer, video camera, etc.) is required to sign a *District Equipment Checkout and Receipt form* acknowledging personal responsibility for the equipment. It is the staff member's responsibility to insure that his/her insurance (typically the "Homeowner's" policy) is sufficient to cover the loss of equipment in the event of theft from personal premises.

The district has a number of hardware resources available for occasional checkout to staff members. Request for these resources is made through the District Technology Department. Borrower's must sign the *District Equipment Checkout and Receipt* form and abide by the same rules as staff members who have been assigned such devices on a permanent basis.

Home Computer Equipment – Installation on School Property

Any staff member who wishes to install personally owned equipment on District property must complete a written request to do so. The required form *(Installation of Staff Owned Equipment on District Premises)* must be completed and submitted to the Technology Department via a Technology Department staff member. Requests are reviewed by the Director of Technology to insure equipment meets network requirements and support the educational objectives of the District. Once approved, the staff member may install his/her personally owned equipment. Personally owned equipment is installed in a school environment AT THE RISK of the staff member. The District has no liability for the loss, theft or damage of personally-owned equipment. The Technology Department DOES NOT provide technical support or supplies for personally owned electronic equipment.

Software Installations – Personally Owned and School Purchased

Employees MAY NOT load any software on District equipment including server drives; only authorized Technology Department staff members may load software. This includes any downloads from the Internet. Requests to have personally owned software installed on classroom or office computers may be submitted in writing to the Director of Technology *(Permission to Use Personal Software on District Equipment* form*)*. Software installation requests that DO NOT violate copyright law and support the educational objectives of the District will be approved and the necessary documentation forwarded to the building Technology Department technology member for installation. Any personally owned software must be MAINTAINED in the classroom (on the school premises) during the period of time that the software is installed on the computer.

Requests to have software purchased with District funds (department, school, PTA budgets, etc.) loaded on classroom computers must be initiated by Technology Department staff members. Appropriate documentation (copy of District Purchase Order, receipt, etc.) must accompany the *Request to Have District-Purchased Software Loaded on District Computer Equipment* form. Once the form and documentation are evaluated by the Director of Technology, approval for installation will be forwarded to the building Technology Department staff member.

District Software Available for Staff Home Use

The district owns a number of software programs that allow for "home" use at no (or reduced) cost to the staff member. Information regarding checkout and/or purchase of free and reduced-cost licenses is available from building Technology Department staff members.

Antivirus Software/OS Upgrades

The Technology Department provides antivirus and operating system security patches at appropriate intervals. In the event of virus infection or security breaches on individual District computers, Technology Department staff members rebuild/reimage computer hard drives to quickly take corrective action. Data stored on an individual hard drive will BE LOST and CANNOT be retrieved. Only data stored on the staff member's server drive (H) is secure.

Reporting Repairs/Service Requests

The procedures for requesting repairs/service related to technology equipment in the District are outlined below:

All Staff Members

All employees requiring technical service must submit an online request for service by accessing the online repair request form:

www.kahoks.org
Departments link
Technology link
General Information link
CUSD Technology Resource Site
All CUSD Submit Support Ticket

The page for service requests is not password protected. If you need assistance with obtaining the username or password required for submitting requests for service, please contact one of the Technology Department staff members in your building.

Administration Building Staff Members

Any employee of the Collinsville Administration Building requiring technical service should contact the Technology Department Support Specialist, Chris Pendleton (cpendlet@kahoks.org; 618-346-6350 ext. 243).

District Technology Staff Members, 2013-2014

Mike Kunz – District
Director of Technology
618-346-6350 ext. 225
mkunz@kahoks.org

Chris Pendleton - District
Technology Department
Support Specialist
618-346-6350 ext. 243
cpendlet@kahoks.org

Derek Turner - District
Network Supervisor
618-346-6350 ext. 226
dturner@kahoks.org

Josh Hartle - CHS
CHS Technician
618-343-4276
jhartle@kahoks.org

Eric Weiss – District
Computer Support Specialist
618-343-2113
eweiss@kahoks.org

Laura Thompson – SPED/District
Computer Support Specialist
618-343-2878
lthomps2@kahoks.org

Chris Oatman – DIS/Renfro/Maryville
Computer Support Specialist
618-346-6311
coatman@kahoks.org

Sherry Murphy – DIS/Renfro/Maryville
Computer Support Specialist
618-346-6265
smurphy@kahoks.org

Geneva Cushing – Caseyville/Twin Echo/Summit/Jefferson
Computer Support Specialist
618-346-6228
gcushin1@kahoks.org

Karen Schemerhorn – Caseyville/Twin Echo/Summit/Jefferson
Computer Support Specialist
618-346-6205
kschemer@kahoks.org

Jane Vlasak – DIS/Renfro/Maryville
Computer Support Specialist
618-346-6261
jvlasak@kahoks.org

Llynn Huntley – Kreitner/Webster/CMS
Computer Support Specialist
618-346-6301
lhuntley@kahoks.org

Jodie Fournigault – Kreitner/Webster/CMS
Computer Support Specialist
618-346-6213
jfournig@kahoks.org

Acceptable Use Policy – Staff Policy

Collinsville Community Unit School District No. 10 Board of Education
Approved: April 20, 1999
Revised: July 15, 2010

Access to Electronic Networks

Terms

The following terms, when used herein, shall be defined as follows for purposes of implementation and administration of this policy:

a. District Electronic Network or Network- the computer hardware and software, including the electronic communications system contained therein which is the property of Collinsville Community Unit District #10.

b. Negligence - the doing of some act which a person of ordinary prudence would not have done under similar circumstances or the failure to do what a person of ordinary prudence would have done under similar circumstances.

c. Data - information and/or documents which are the property of Collinsville Community Unit District #10, a staff member, or a student thereof and which an employee does not otherwise have normal access to or use of as part of her/his normal employment duties. The term "data" shall not refer to such items as tests, worksheets, material normally assigned to or distributed to students or staff by the employee as part of his/her normal employment duties, student records maintained by the employee, student grades assigned by the employee, or other curricular and extracurricular material normally prepared and used by the employee during the course of her/his normal employment duties.

Overview

Electronic networks, including the Internet, are a part of the District's instructional program in order to promote educational excellence by facilitating resource sharing, innovation, and communication. The Superintendent or designee shall develop an implementation plan for this policy.

The School District is not responsible for any information that may be lost, damaged, or unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet. The District may hold the user responsible for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of the *Personnel Access To Electronic Networks and Acceptable Use Policy.*

Curriculum

The use of the District's electronic networks shall (1) be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students, and (2) comply with the selection criteria for instructional materials and library-media center materials. Staff members may, consistent with the Superintendent's implementation plan, use the Internet throughout the curriculum.

The District's electronic network is part of the curriculum and is not a public forum for general use.

Compliance with Copyright Laws

The Board of Education intends to adhere to all copyright laws as applied to computer software. The Board also intends to comply with the license agreements and/or policy statements contained in the software packages used in the District. Therefore, all software used on District computers or computer networks shall be purchased by the Board, properly licensed and registered with the publisher, and installed by the Director of Technology or other designated personnel.

Acceptable Use

All use of the District's electronic network must be (1) in support of education and/or research, and be in furtherance of the School Board's stated goal, or (2) for a legitimate school business purpose. Use is a privilege, not a right. Students and staff members have no expectation of privacy in any material that is stored, transmitted, or received via the District's electronic network or District computers. General rules for behavior and communications apply when using electronic networks. The District's *Personnel Access To Electronic Networks and Acceptable Use Policy* contains the appropriate uses, ethics, and protocol. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

Internet Safety

Each District computer with Internet access shall have a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee. The Superintendent or designee shall enforce the use of such filtering devices. An administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose, provided the person receives prior permission from the Superintendent or system administrator. The Superintendent or designee shall include measures in this policy's implementation plan to address the following:

1. Limiting student access to inappropriate matter as well as restricting access to harmful materials;

2. Student safety and security when using electronic communications;

3. Limiting unauthorized access, including "hacking" and other unlawful activities; and

4. Limiting unauthorized disclosure, use, and dissemination of personal identification information.

Authorization for Electronic Network Access

Each student and his or her parent(s)/guardian(s) must sign the *Authorization* before being granted access to the District's Electronic Network. All use of the District's Electronic Network shall be consistent with the District's goal of promoting education excellence by facilitating resource sharing, innovation, and communication. This policy does not attempt to state all required or prescribed behavior by users. However, some specific examples are provided. The failure of any user to follow the terms of the *Personnel Access To Electronic Networks and Acceptable Use Policy* may result in the loss of privileges, disciplinary action in accordance with the applicable provisions of the appropriate collective bargaining agreement, and/or appropriate legal action. Users shall be subject to disciplinary action under this policy only after they have been given a copy of this policy. Employees will be required to give a signature acknowledging receipt of a copy of this policy.

All users of the District's computers and means of Internet access shall maintain the confidentiality of student records. Reasonable measures to protect against unreasonable access shall be taken before confidential student information is loaded onto the network.

Use of Unauthorized Software/Unauthorized Copying of Software

a. Staff members shall not be permitted to load or copy software (District-owned or personal) without the express written permission of the Director of Technology or designee. All software used on District computers or computer networks shall be, properly licensed and registered, and installed by the Director of Technology or designee.

b. Staff members shall not be permitted to copy any District owned software without the express written permission of the Director of Technology or designee.

Unauthorized Access/Sharing Passwords

a. Staff members shall not tamper with, attempt to gain or gain access to computer data to which a staff member has no security authorization (such as, but not limited to, financial, employee, and student information). All staff members are prohibited from intentionally or negligently allowing students or other individuals (such as, but not limited to, friends, relatives, District employees, etc.) to access or update information under their network login name and password.

b. All staff members are prohibited from sharing stand-alone computer and/or network login names and passwords. Passwords must be kept confidential and should be changed at regular intervals. Minimum is every 365 days.

Modifying, Damaging, Destroying or Copying of Data

a. Staff members shall not in any manner modify, damage, destroy, or copy any data belonging to the School District or any staff member or student thereof without express written permission from the Director of Technology or designee.

b. Any staff member who vandalizes or otherwise intentionally damages any District hardware or software, shall be responsible for payment of all repair, service and/or replacement costs.

c. Staff members shall not attach any external devices to the District network without prior written approval from the Director of Technology or designee.

Unacceptable Use

Employees of the District are responsible for their actions and activities involving the District Electronic Network and Internet. Examples of unacceptable use include:

a. Intentionally using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State regulation;

b. Downloading copyrighted material for other than personal use;

c. Using the network or District equipment for commercial gain;

d. Invading the privacy of individuals;

e. Using another user’s account or password;

f. Intentionally posting material authored or created by another without his/her consent;

g. Intentionally posting anonymous messages;

h. Partisan political activities; campaigning for or against public policy questions that appear on a ballot; promoting election issues or candidates for collective bargaining units;

i. Intentionally accessing, submitting, posting, publishing or displaying any defamatory, abusive, obscene, profane, pornographic, threatening, racially offensive, harassing or illegal materials, and material of a sexual nature that is inappropriate in a school environment;

j. Authoring and/or editing, FROM SCHOOL DISTRICT EQUIPMENT OR USING THE DISTRICT NETOWRK, district or personal web pages that contain any nudity or pornography; copyright infringement; material that is threatening, abusive, harassing, defamatory, invasive of privacy or publicity rights, vulgar, obscene, profane, indecent, or otherwise objectionable; content that promotes, encourages, or provides instructional information about illegal activities---specifically hacking, cracking, or phreaking, including posting other peoples' or district private information; and any software, information, or other material that contains a virus, "Trojan Horse", "worm" corrupted data, or any other harmful or damaging component; hate propaganda or hate mongering, swearing, or fraudulent material or activity; and

k. Using the network while access privileges are suspended or revoked.

l. Using the Network to perform any acts of cyber-harassment or cyberstalking (as defined by Illinois Compiled Statutes 720 ILCS 135 Harassing and Obscene Communications Act. Section 1 **(720 ILCS 135/1-2)**

Staff Use of Electronic Mail Communication

Electronic mail communication using District email addresses shall be used for educational or school business purposes only. Staff shall not be allowed to use the School District’s electronic mail communication for personal messages, anonymous messages or communications unrelated to an education or school business related issue. Staff shall not use electronic mail communication to create, communicate, repeat or otherwise convey or receive any message or information which is illegal, indecent, obscene, harmful to minors, inappropriate for minors, child pornography, defamatory, likely to constitute harassment of another student, staff member or any other individual, likely to cause disruption in the schools, or is otherwise inconsistent with the District’s curriculum and educational mission.

Staff shall respect the privacy rights of others and shall not attempt to access any electronic mail communications not directed to them or intended to be received by them unless for a legitimate and bona fide educational reason or safety precaution, and as directed by the Superintendent or his/her designee.

Violations

The failure of any student or staff member to follow the terms of this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

Any staff member who violates the *Personnel Access To Electronic Networks and Acceptable Use Policy* shall be subject to disciplinary action up to and including dismissal in accordance with the applicable provisions of the appropriate collective bargaining agreement and/or The School Code. The Superintendent or designee and/or the Building Principal will make all decisions regarding whether or not a user has violated the *Personnel Access To Electronic Networks and Acceptable Use Policy* and may deny, revoke or suspend access at any time. A user who disagrees with a decision made by the Superintendent, designee, and/or the Building Principal regarding whether or not a user has violated the *Personnel Access To Electronic Networks and Acceptable Use Policy* may appeal such decision through the grievance procedure of the appropriate collective bargaining agreement.

Additionally, if staff member conduct constitutes a violation of copyright laws, the staff member may be subject to prosecution under such laws. Any staff member who intentionally or negligently damages or destroys District hardware and/or software shall also be responsible for all costs associated with repair and/or replacement parts and services.

LEGAL REF.: Children's Internet Protection Act, P.L. 106-554., 20 U.S.C § 6801 et seq., 47 U.S.C. § 254(h) and (l), 720 ILCS 135/0.01.

CROSS REF.: 5:100 (Staff Development Program), 5:170 (Copyright for Publication or Sale of Instructional Materials and Computer Programs Developed by Employees), 6:40 (Curriculum Development), 6:210 (Instructional Materials), 6:230 (Library Resource Center), 6:260 (Complaints About Curriculum, Instructional Materials, and Programs), 7:130 (Student Rights and Responsibilities), 7:190 (Student Discipline), 7:310 (Publications)

ADMIN PROC.: 6:235-AP (Administrative Procedure - Access to Electronic Networks), 6:235-E2 (Exhibit - Authorization for Electronic Network Access)

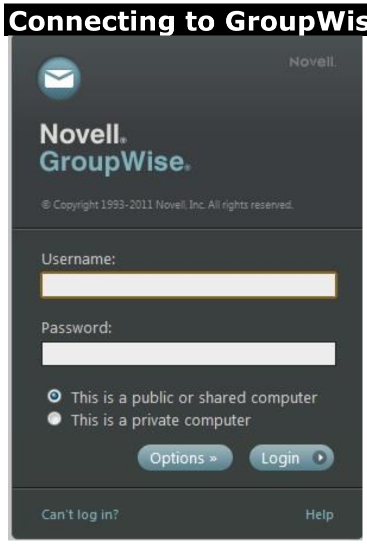
APPROVED: April 20, 1999

REVISED: July 11, 2013

Using GroupWise WebAccess

You can access your GroupWise mailbox from home or another remote location through a web browser such as Internet Explorer. The GroupWise WebAccess interface looks different than your **CUSD10 desktop** GroupWise version.

Connecting to GroupWise WebAccess


Novell.
Novell.
GroupWise.
© Copyright 1993-2011 Novell, Inc. All rights reserved.
Username:
Password:
● This is a public or shared computer
○ This is a private computer
Options »
Login
Can't log in?
Help

1. Open your web browser.
2. Go to: www.kahoks.org
3. Click on the **Employees** link.
4. Click on the **Email Access** link.
5. Click on the **Check Your District Email Account Here** link in the Resource Directory section.
6. Enter your Username and Password (passwords are case sensitive).
7. Click on the **LOGIN** button.

Note: If you do not perform any actions in GroupWise WebAccess for a period of time you may have to log back in.