

Collinsville Community Unit School District No. 10

## **Technology Department**

### **General Guidelines and Procedures For Staff Access to Electronic Resources**



**2011-2012**

© August 2009 - Collinsville CUSD10

## Table of Contents

Section Title	Page
Procedures for Requesting Network Access	2
Data Storage and Server Account	3
Accessing Server Data from Another District Location	4
Accessing Server Data from Home	6
Email Account	14
Web Access to Email Account	15
If an employee uses America Online...	16
Requesting Publishing of Email Address on District Web Site	16
Internet Access and Internet Filtering	16
Copyright	18
Staff Web Pages	18
District Equipment Checkout	19
Home Computer Equipment – Installation on School Property	19
Software Installations – Personal Owned and School Purchased	20
District Software Available for Staff Home Use	21
Antivirus Software/OS Upgrades	21
Reporting Repairs/Service Requests	21
District Technology Staff Members, 2005-2006	23
District Acceptable Use Policy – Staff Policy	24
GroupWise 8.1 WebAccess Quick-Start Guide	32

Collinsville Community Unit School District No. 10  
Technology Department

**General Guidelines for Network Access, Internet  
Access and Email**

2011-2012

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](http://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. 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.

The District uses 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 MAY NOT save data or documents to any District computer's hard drive without written permission from the Director of Technology.** 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 CD-Rom, if available). Documents and data stored to a computer's hard drive are NOT SECURE from other users. District computers protection software automatically deletes any documents or software saved to a computer hard drive upon reboot. These documents CANNOT be retrieved once a computer has been rebooted.

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.

**Critical data, such as electronic grade files, should be saved in two locations for the greatest security.** For example, teachers choosing to use *Grade Book* for recording and processing student grades should store data on both the server drive (H) and USB key drive or other media.

### **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.

The majority of employees have server accounts only at their home schools. Therefore, an employee who is working or visiting another school could not, in theory, access the network or the Internet at that location. 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).

To log in remotely from a school (other than the employee's home school), follow the three steps outlined below:

Periods (.) before and after the User Name is critical to remote login success.

1. In the "**User Name**" box, type (NO spaces):

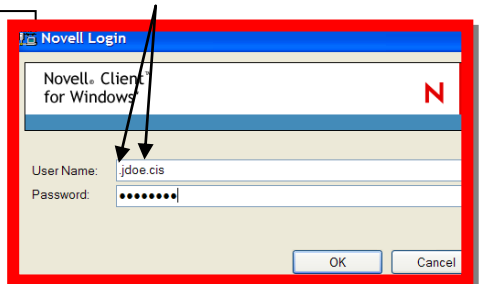
- a PERIOD (.)
- the employee Novell User Name (for example, **jdoe**)
- Another PERIOD (.)
- the school server name (see *list below*)

**Examples by school (w/server name)**

Admin - .jdoe.admin

Caseyville - .jdoe.caseyville  
Hollywood - .jdoe.hollywood  
Jefferson - .jdoe.jefferson  
Kreitner - .jdoe.kreitner  
Maryville - .jdoe.maryville  
Renfro - .jdoe.renfro  
Summit - .jdoe.summit  
Twin Echo - .jdoe.twinecho  
Webster - .jdoe.webster

CIS - .jdoe.staff\_teachers.cis  
CMS - .jdoe.staff\_teachers.cms  
CHS - .jdoe.chsstaff.groupwise



2. Once the **User Name** box has been completed correctly, type the normal password.
3. Click **OK**

Note: Logging into a remote school with your User Name may cause printing problems. If you are logging into a computer with a printer directly attached via USB or Parallel port, printing will be possible.

For additional assistance with remote login, contact a Technology Department staff member.

## **Accessing Server Data from Home**

Employees may access data stored in their school network account 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](http://www.kahoks.org)
2. Click on **Departments**
3. Click on **Technology**
4. Click on **General Information**
5. Click on the **"Access District Server Account"** link (first link under the heading "Resource Links")
6. Enter your username. **You must enter the complete context of the building server you have your files stored on.** Your personal context will be your login name followed by a period (.) followed by your building server name. Server names are listed here:

Yourlogin.admin	Admin Building and Warehouse employees
Yourlogin.caseyville	Caseyville employees
Yourlogin.hollywood	Hollywood Heights employees
Yourlogin.jefferson	Jefferson employees
Yourlogin.kreitner	Kreitner employees
Yourlogin.maryville	Maryville employees
Yourlogin.renfro	Renfro employees
Yourlogin.summit	Summit employees
Yourlogin.twinecho	Twin Echo employees
Yourlogin.webster	Webster employees
Yourlogin.staff_teachers.cis	DIS employees
Yourlogin.staff_teachers.cms	CMS employees

Yourlogin.chsstaff.groupwise
------------------------------

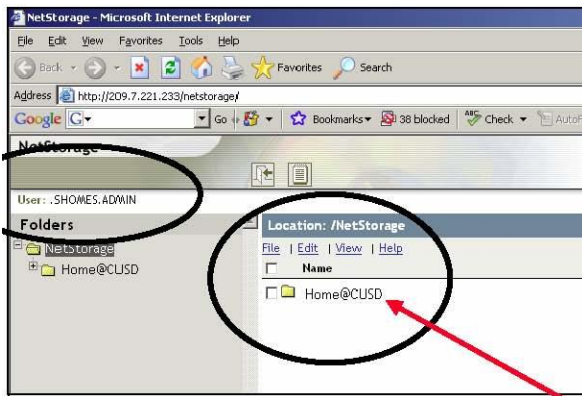
CHS employees
---------------

For example, if my login name was jdartmer and I worked at DIS, I would type the following as my remote login name:

jdartmer.staff\_teachers.cis

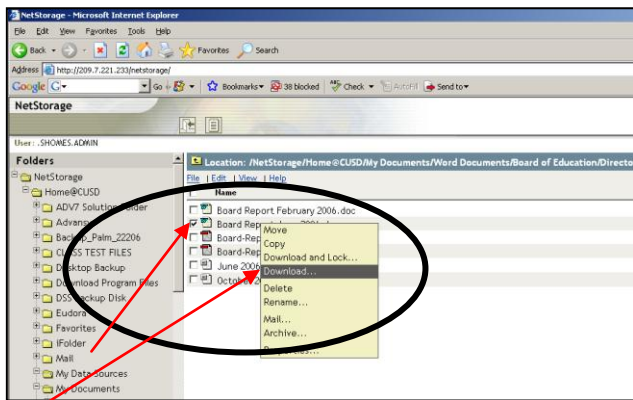
7. Enter your Novell password
8. Press ENTER

After a successful login, the remote NetStorage screen will look like this. The folder named Home@CUSD represents your H drive at school. You may double-click this folder to expand it and view the contents.

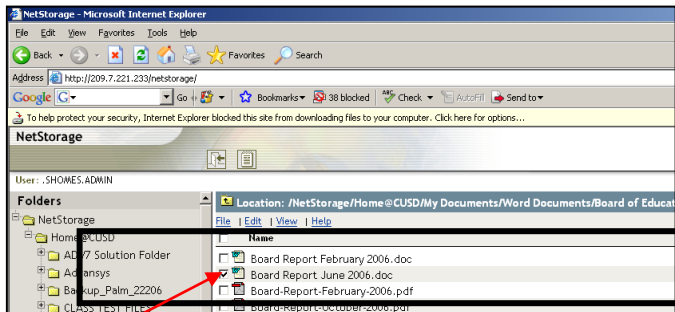


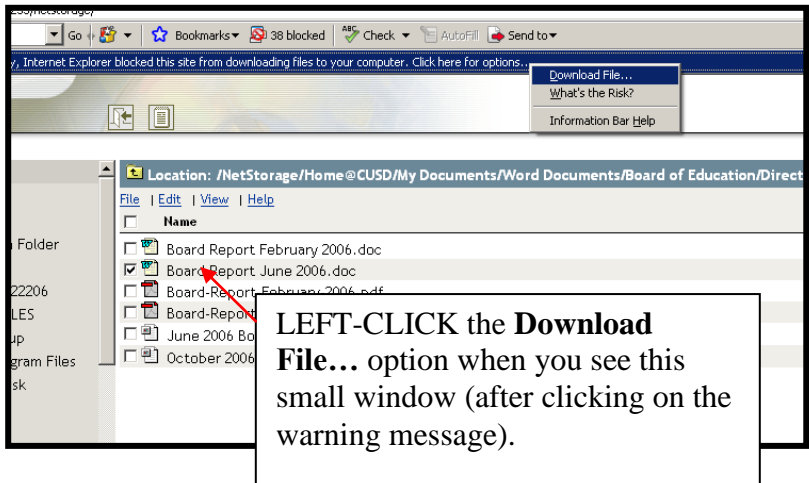
## Downloading files from your district network account to your home computer

1. Once you navigate to the folder and file that you wish to work with at home or outside the district, RIGHT-CLICK your mouse over the file name. This will automatically place a checkmark to the left of the file and present you with a small menu of options. LEFT-CLICK on the **Download...** option.

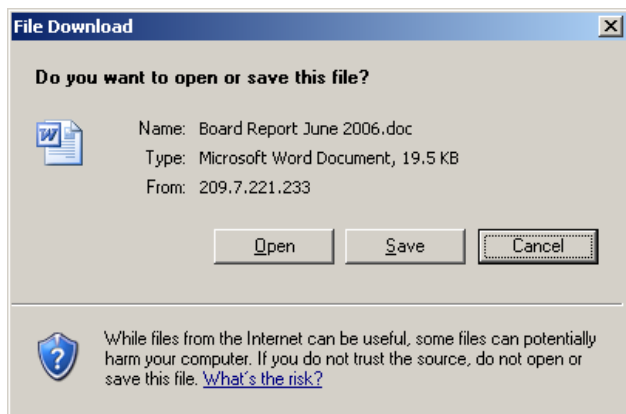


2. Depending on the browser and level of security you have set on your computer, you may have to allow the downloading of the file by clicking on the warning bar below your browser's address bar:





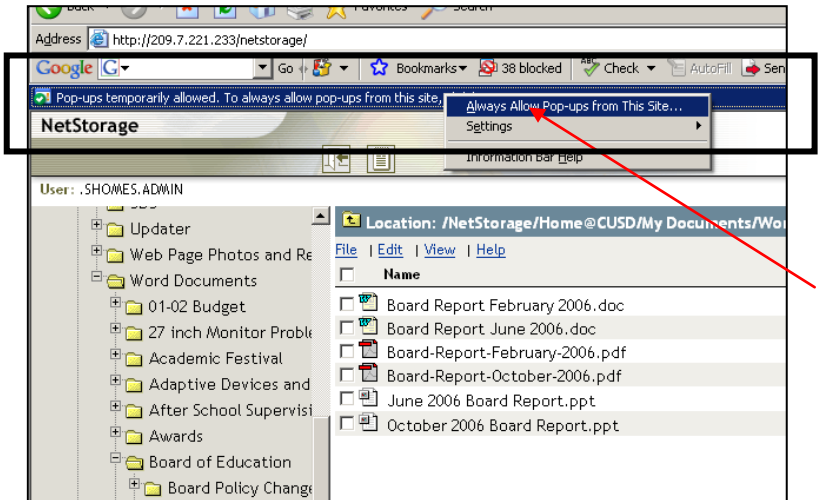
3. You can now click on the **Save** feature and choose your destination. Many people choose their computer "desktop" for the destination to increase speed in finding and working with the file after it has been downloaded.



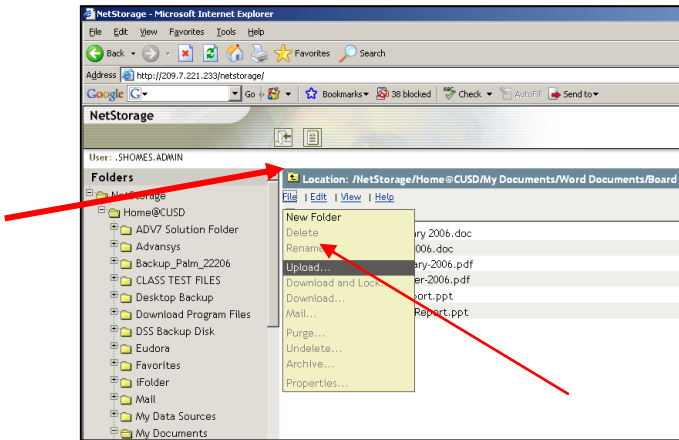
## Uploading files or changes to your district network account from your home computer

If you plan to make changes to the file at home (or on a remote computer) and want to move a copy of the changes to your district server account, you will then need to **UPLOAD** the file to your H drive using the NetStorage window. To upload a changed or new file to your server drive, follow these steps:

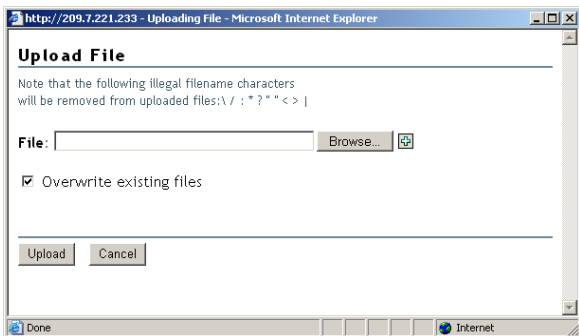
1. Temporarily ALLOW popups on your computer. This is required to upload files via NetStorage on the web.



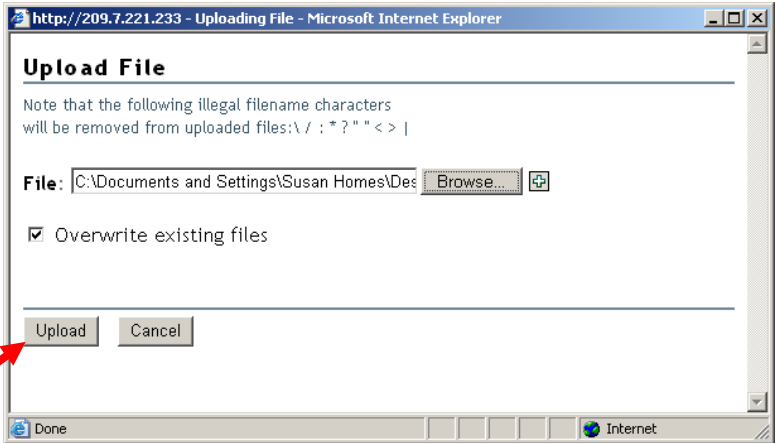
Using the **NetStorage** window, navigate to the area of your server directory where you wish the uploaded (changed or new) file to be stored. Click on **File...Upload...**



**Click on the Browse...** button to search for the file you wish to upload. It will be located on your home (or remote computer). If the file you plan to upload is replacing the old copy on your server directory, be sure the "Overwrite existing files" option is checked. If you are uploading a new file or another copy of your original file (with a different name), you can remove the check from this box.

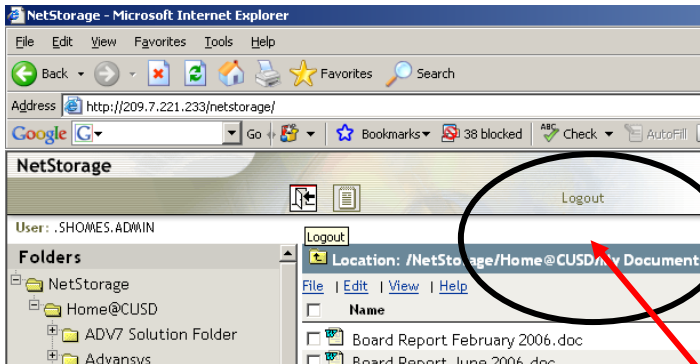


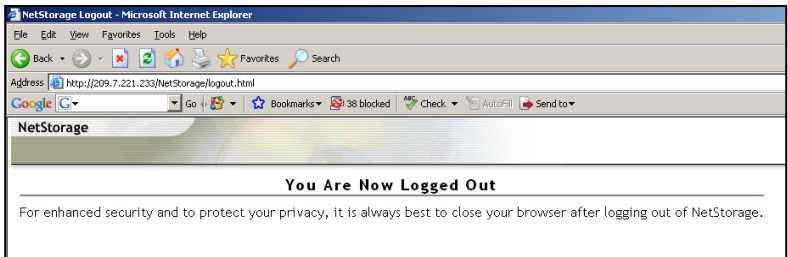
Once you have located the file and it appears in the **"File"** locator box, click the **Upload** button.



### **Logging Out of NetStorage**

It is critical that you properly logout of NetStorage when you are finished accessing or uploading to your district network account. Not exiting properly puts your district data at risk to other users of your home (or remote computer). It is your responsibility to protect your data at all times.





## **Warnings:**

If you download a file to work with at home or remotely, it is important to remember that you must **UPLOAD** the file if you have made changes to it and wish to have those changes reflected when you get back to school.

When you open a downloaded file at home (or remotely) and click on the **SAVE** option within the program (such as Word, PowerPoint, etc.), the saved changes apply only to the copy that you have downloaded to your home computer. These changes **DO NOT** automatically apply to the copy of your document on your school server account. You must **UPLOAD** the edited file to your server account to insure the copy you have at school includes your changes.

Please contact a technology staff member for additional assistance if you have any questions.

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 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](mailto:_____@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 Retain. The Retain 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 Retain program:

1. Navigate to [www.kahoks.org](http://www.kahoks.org)
2. Click on **Employees link**
3. Click on **Email Access link**
4. Click on **Access Email archive system**
5. Enter you username and password.

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. Once an employee has been assigned a District email account, he/she may contact a Technology Department staff member for assistance in hard-coding the email password so that web access will be functional on the account.

To access the email account via the Internet:

[www.kahoks.org](http://www.kahoks.org)

Employees link

Email Access link

Check Your District Email Account Here link

(Resource Directory)

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](http://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."**

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.

Students must be monitored by District personnel **at all times** while they are accessing the Internet. 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 Shutterfly.com. 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, 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. 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](http://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 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, 2011-2012**

**Mike Kunz - District**  
Director of Technology  
618-346-6350 ext. 225  
[mkunz@kahoks.org](mailto:mkunz@kahoks.org)

**Chris Pendleton - District**  
Technology Department  
Support Specialist  
618-346-6350 ext. 243  
[cpendlet@kahoks.org](mailto:cpendlet@kahoks.org)

**Derek Turner - District**  
Network Supervisor  
618-346-6350 ext. 226  
[dturner@kahoks.org](mailto:dturner@kahoks.org)

**Josh Butler - CHS**  
CHS Technician  
618-343-4276  
[jbutler@kahoks.org](mailto:jbutler@kahoks.org)

**Eric Weiss - CMS** Computer  
Support Specialist  
618-343-2113  
[eweiss@kahoks.org](mailto:eweiss@kahoks.org)

**Laura Thompson - DIS**  
Computer Support Specialist  
618-346-6311  
[lthomps2@kahoks.org](mailto:lthomps2@kahoks.org)

**Karen Schemerhorn -  
Caseyville**  
Computer Support Specialist  
618-346-6205  
[kschemer@kahoks.org](mailto:kschemer@kahoks.org)

**Ruth Hawkins -  
Jefferson & Summit**  
Computer Support Specialist  
618-346-6214 (Jefferson) & 618-  
346-6221 (Summit)  
[rhawkin1@kahoks.org](mailto:rhawkin1@kahoks.org)

**Jodie Fournigault - Kreitner**  
Computer Support Specialist  
618-346-6213  
[jfournig@kahoks.org](mailto:jfournig@kahoks.org)

**Jane Vlasak - Maryville**  
Computer Support Specialist  
618-346-6261  
[jvlasak@kahoks.org](mailto:jvlasak@kahoks.org)

**Sherry Murphy - Renfro**  
Computer Support Specialist  
618-346-6265  
[smurphy@kahoks.org](mailto:smurphy@kahoks.org)

**Geneva Cushing - Twin Echo**  
Computer Support Specialist  
618-346-6228  
[gcushin1@kahoks.org](mailto:gcushin1@kahoks.org)

**Lynn Huntley - Webster**  
Computer Support Specialist  
618-346-6301  
[lhuntley@kahoks.org](mailto:lhuntley@kahoks.org)

## **District Acceptable Use Policy – Staff Policy**

Collinsville Community Unit School District No. 10 Board of Education

Approved: April 20, 1999

Revised: July 15, 2002

### **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 - 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 *Access To Electronic Networks*.

## 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 *Authorization for Electronic Network Access* 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 *Access To Electronic Networks* 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.

### 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.

### 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 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, 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/or

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

### 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 *Access To Electronic Networks* 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 *Access To Electronic Networks* 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 *Access To Electronic Networks* 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 REFERENCES:

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.

## 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.

Your GroupWise account must be set up BEFORE you attempt to use GroupWise WebAccess. **In addition, you must hardcode your password through the desktop GroupWise client on a CUSD computer.** Contact the Technology Department staff member in your building for assistance with these **critical steps**.

## Connecting to GroupWise WebAccess



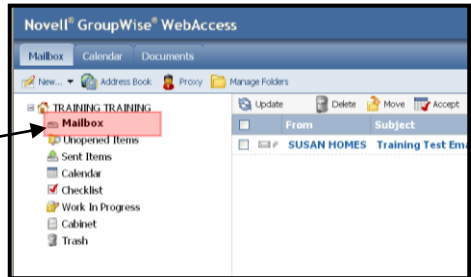
1. Open your web browser.
2. Go to: [www.kahoks.org](http://www.kahoks.org)
3. Click on the **Employees** link.
4. Click on the **Email Access** link.
5. Click on the **Check Your District Email Account Here** link in the Resource Directory section.
6. Enter your Username and Password (passwords are 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 will have to log back into the system.

## Reading Email

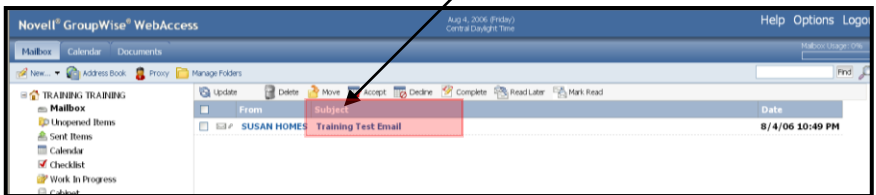
When you first log in, your **Mailbox** should be visible. If you have moved to another GroupWise window, you can return to your Mailbox as follows:

1. Click on **Mailbox** in the **Folder List** on the left side of your screen.



To read an email:

1. Click on the **Subject** heading of the email listing. **You must have any pop-up blockers temporarily disabled on your computer** to allow the message window for your emails to appear.
2. You can reply to, forward, delete, etc., the message by clicking on the appropriate button at the top of the message window.

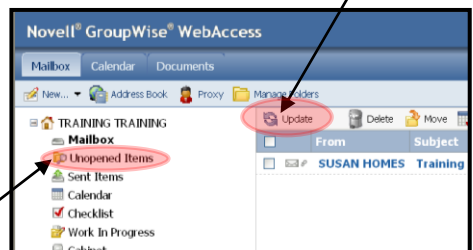


By default, 20 messages at a time can be displayed in your WebAccess mailbox. If you have more than 20 messages, a **Display Next** button appears at the bottom of the screen. Click on this button to see the next group of messages.

## Updating the Screen

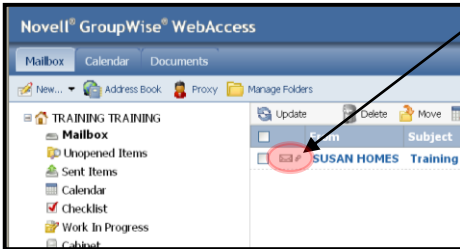
Because of web browser limitations, if messages are added, deleted, or moved from your mailbox, these changes may not be immediately apparent. To refresh your screen:

Click on the **Update** link above your messages or click on the **Unopened Items** link in the **Folder**



**List** on the left side of your screen.

## Opening and Saving an Attached File

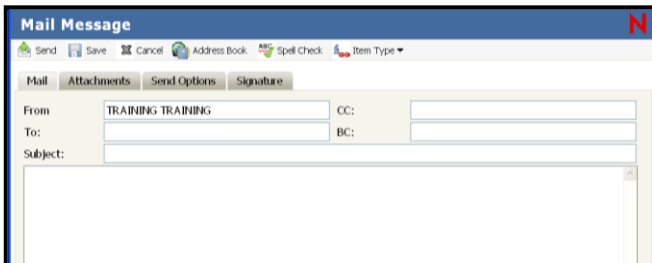


If a message has an attachment, a paperclip icon appears to the left of the **Subject** heading for an email. To view the attachment:

1. Open the message. The attachment is listed under the message subject. Options appear at the end of the attachment name.
2. Click on **View** to look at the attachment with the GroupWise viewer; or click on **Save As** to save the file to a desired location on your computer such as the desktop or your network drive.

## Creating and Sending a Message

1. Click on the **New** icon on the left side of your screen.
2. Type the recipient's email address in the "To" field. If sending to more than one person, separate each address with a comma. You can also look up addresses in the Address Book.

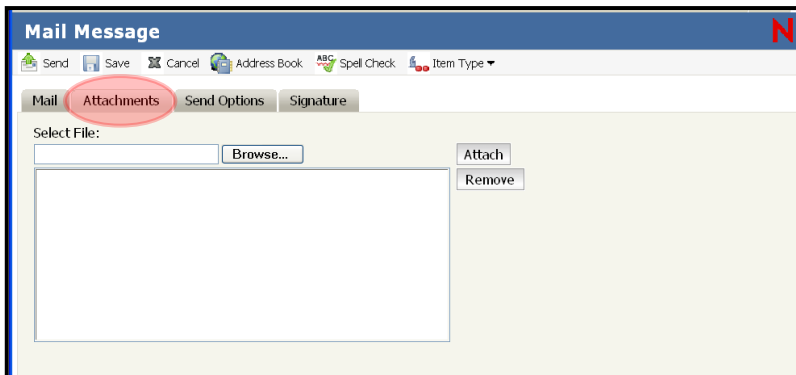


3. Run the **Spell Check** and set any desired options.
4. Click on **Send** when you are ready to transmit your message.

## Attaching a File

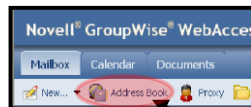
1. Click on the **Attachments** tab in the message window.

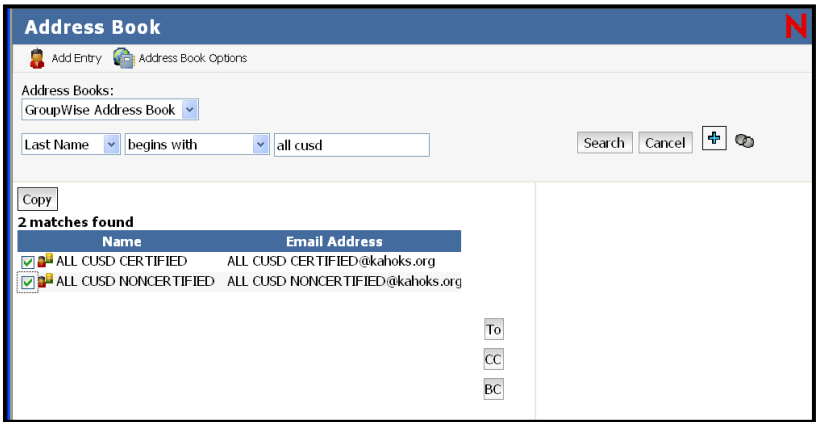
2. Click on **Browse** and locate the file.
3. Double-click on the filename.
4. Click on **Attach**.
5. Repeat Steps 2-4 (above) to attach additional files.
6. Click on **Send** to transmit the message with the attachment or click on the **Mail** tab to return to the message window before sending the email.



## Using the Address Book

1. Click on the Address Book icon on the menu bar near the top of the screen or in the Mail Message window.
2. Select the desired address book (Groupwise Address Book is the general listing of all employees; this list can only be modified by the network manager. Frequent Contacts is the address book that contains an employee's email "frequent" or personally-added contacts).
3. From the drop-down list, select a category such as "Last Name."
4. Select a type of search such as "Begins with."
5. In the text box, type the first few letters of the name you are trying to locate.
6. Click on the **Search** button.
7. Once the desired name appears, place a checkmark in the box to the left of the name.
8. Click **TO:** **CC:** or **BC:** to address a message (or copy a message) to the desired recipients.
9. Click **OK** to continue with the message window.

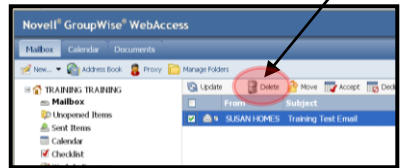




## Deleting Messages

To delete a message, open it and click on the **Trash Can (Delete)** at the top of the message window OR do the following:

1. In the Mailbox list, check the box to the left of the message(s) to be deleted.
2. Click on the **Trash Can (Delete)** at the top of the screen or press the Delete key on the computer keyboard.



Deleted messages go into the Trash folder. From there, you can remove messages one at a time or all at once.

Messages in the trash will be deleted after approximately 30 days.

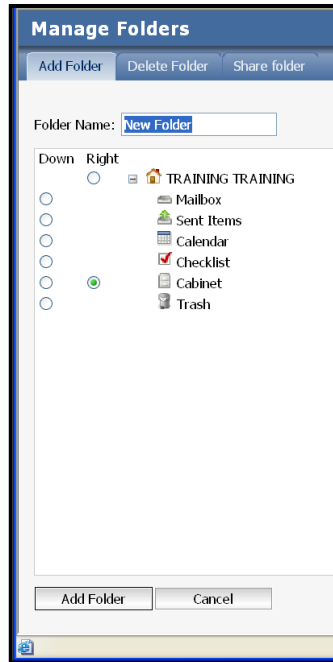
## Creating Folders

You can create folders in which to store and organize your messages. To create a folder:

1. Click on **Manage Folders** near the top of the screen.
2. Enter a name for the folder.

- Click on the radio button to the left of the **Mailbox** line to make the new folder easily viewable in the **Mailbox** listing.
- Click **Add Folder**.

The **Manage Folders** window also allows you to delete folders and set up folders to share contents with other district users. When sharing folders with others, they will receive an individual email inviting them to accept the shared folder and determine where in their own **Mailbox** listing the folder will appear.



Long-term storage of messages in the standard GroupWise

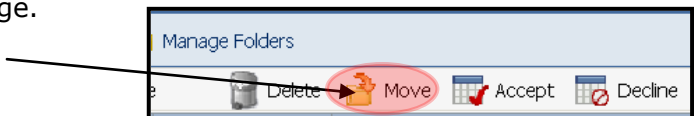
**Folder List** is not recommended. Each user's mailbox size is limited. Storing messages in the **Folder List** will decrease the amount of space you have for incoming messages and may eventually lead to a "full" mailbox. Users should **archive** messages they wish to save (described later).

## Moving Messages

To move a message that you are reading, click on **Move** at the top of the message window OR

To move messages from the main Mailbox window:

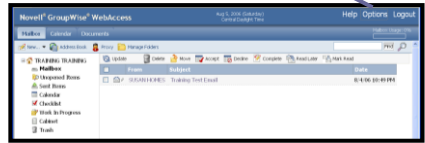
- Check the box in front of the message(s) that you wish to move.
- Click on **Move** at the top of the message window.
- Click on the folder where you would like to store the message.



**Setting an Email**

**Signature**

1. Click on the word **Options** at the top (right-hand) of your screen.
2. Click on the **Signature** tab.
3. Type your desired signature in the text box provided.
4. Place a checkmark in the **Activate signature** box.
5. Choose the **Automatically add signature** option.
6. Click **Save**.



**Options** N

General Password Proxy Access Rules Send Options **Signature** Time Zone

**Add your signature to outgoing messages**

Activate signature

Jones Johnson  
Director of Instructional Services

Automatically add signature

Prompt before adding signature

Save Close

## Creating a Vacation Rule

If you will be unavailable for a period of time due to leave, vacation, etc., you may wish to set up a **Vacation Rule** that will automatically send a reply to messages that arrive in your Mailbox while you are gone.

**Options** N

General Password Proxy Access **Rules** Send Options Signature Time Zone

Type: Vacation Create

Save Close

### To set up a **Vacation Rule**:

1. Click on the word **Options** at the top (right-hand) of your screen.

2. Click on the **Rules** tab.
3. Click on **Create**.
4. Type a **Rule Name**.
5. Type a **Message**; click **SAVE**.
6. Insure that a checkmark is in the box to the left of the new rule.
7. Click **Save**.

## Exiting WebAccess

Click on the word **Logout** at the top (right-hand) of your screen to exit GroupWise WebAccess.

Help Options **Logout**

