

Diocese of Columbus Office of Catholic Schools Guide to Computing Resources

Updated 4/3/2006

The Office of Catholic Schools provides two major computing resources to the faculty, staff, and students of its schools: access to internet E-mail, and access to information via the Office of Catholic Schools web site. Both of these resources will be covered in detail in the following chapters.

There is an acceptable use policy that governs proper use of the computing resources provided by the Office of Catholic Schools. Please request a copy from your school's technology coordinator before using these services.

Table of Contents

I) E-mail	2
A) Overview.....	2
B) Logging in to the diocesan system	2
1) The traditional terminal interface.....	2
2) The web browser interface.....	4
3) POP3/IMAP client program interfaces (Outlook Express, Eudora, etc.).....	4
C) E-mail quotas.....	5
D) Security, Privacy, Spam, and Viruses.....	5
1) Security.....	5
2) Privacy.....	5
3) Spam.....	7
4) Viruses.....	7
II) World Wide Web Services	9
A) Public Information.....	9
B) Resources for teachers and staff.....	9
III) Appendices	10
A) Appendix A: Configuring SSH for Windows.....	10
B) Appendix B: Configuring MacSSH for Macintosh.....	10

I. E-mail

A) Overview

Employees of diocesan schools are provided with an e-mail account on the “Clarus” e-mail system. This account can be used to communicate with other people in the diocese, as well as with others on the internet. E-mail addresses for users of the diocesan system take the form of username@cdeducation.org.

B) Logging into the diocesan e-mail system

Once you are provided with an account name and initial password, you can begin using the e-mail system. The e-mail system can be accessed in one of three ways:

- 1) the traditional terminal interface (Pine)
- 2) the web browser interface (Webmail)
- 3) 3rd-party client program interfaces (Outlook, Eudora, etc.)

1) The traditional terminal interface (Pine)

Use any standard SSH (secure shell) application to connect to the e-mail server. The server name is **cdeducation.org**. Enter your login name and password when prompted. Once you are logged in, the “Pine” e-mail program can be started by selecting the first item on the menu. When you are done, the last item on the menu will log you out of the system.

For a tutorial on using the Pine e-mail program, please visit the following site:
www.washington.edu/pine/tutorial.4/index.html

Although Pine may appear to provide support for saving or sending attachments (such as graphics or sound files), these functions will not work via the terminal interface. If you need to send or receive an attachment, use the Webmail interface instead (see below).

Depending on the terminal program you use to connect to the e-mail server, some functions may not be available (such as printer support). For full access to all the features of Pine, the Office of Catholic Schools recommends the use of **SSH Secure Shell** for Windows users and **MacSSH** for Mac users. Both products are free for non-commercial use. Please see **Appendix A** or **B** if you need either of these programs.

Pine is not the only program available through the terminal interface. You can also perform account maintenance, such as setting up mail filters to block unwanted e-mail. You can also change your password or look up the addresses of other users of the diocesan e-mail system.

2) The web browser interface (Webmail)

Use any standard web browser (Firefox, Internet Explorer, etc.) to connect to the diocesan server. The address is www.cdeducation.org/webmail . Enter your username and password in the appropriate boxes and click the “Login” button.

The webmail application can also send and receive files as attachments to e-mail messages. To save an attachment sent to you, click on the “download” link next to the name of the attachment.

Online help is available by clicking the “Help” link after logging in.

3) POP3/IMAP client program interfaces (Outlook Express, Eudora, etc.)

Use any standard POP3/IMAP client program, such as Outlook Express or Eudora, to connect to the e-mail server. Both the SMTP and POP3/IMAP server names should be set to **cdeducation.org** . * You may select either POP3 or IMAP access. POP3 will download your mail to your local computer when you log in, so take care if you use this on multiple computers or shared computers. Choosing IMAP will leave your mail on the central server so you can still access it from other computers. **NB:** Using IMAP on non-school computers may require performing an additional step to configure. Please see your technology coordinator for details.

The diocesan e-mail server may require you to check your inbox for new mail before you are able to send mail. If you receive an error message stating that “relaying is denied” when you try to send mail, please have your software check for new mail first, and then try sending your message again.

If you need further help with your POP3 or IMAP client program, please consult its documentation.

* Some ISP’s have chosen to block connections to SMTP servers not under their control. If this is the case with your ISP, attempting to send messages will always result in an error. To remedy this, please change your SMTP server setting to match your ISP’s official SMTP server name.

C) E-mail quotas

Each user of the diocesan e-mail system is allocated 128MB of disk storage space. Quota usage can be checked by logging in to **cdeducation.org** via the terminal interface (see **the traditional terminal interface** above). The usage summary is displayed prior to the main menu, or by selecting option "L" from the main menu. You will also be notified via e-mail if you have exceeded your limit.

Storage of large multimedia graphics or sound files as “attachments” in your e-mail folders is not recommended and will significantly impact the amount of free space in your account. Once these attachments are downloaded to your hard drive, the original e-mail messages containing them can be deleted to free up space in your account. If the amount of mail in your account exceeds 128MB, you will be unable to receive any more messages, and anyone trying to e-mail you will receive a delivery error. To fix this situation, you must delete some messages. (If you use Webmail, remember to empty the DELETED folder; if you use Pine, remember to press “Q” to quit. Otherwise, deleted messages may still take up space in your account.)

Additionally, the diocesan e-mail system must not be used to distribute very large attachments to multiple users of the system, as this puts a heavy load on the server and can overflow quotas.

D) Security, Privacy, Spam, and Viruses

1) Security

All users of the Office of Catholic Schools' e-mail system are required to select a new password every 90 days. Users will receive an e-mail message when it is time to start thinking of a new password. Users who access the system via the terminal interface will also receive an additional reminder upon login. After 90 days plus a short grace period, the account will be "locked" if the password has not yet been changed. If your account has been locked, or if you have forgotten your password, please see your technology coordinator for a new password.

Although this policy may seem inconvenient, changing system passwords helps to insure the security of your account. It also prevents stale accounts from being used fraudulently by anyone who discovers the password.

Passwords may be changed by either logging into Clarus via the terminal interface, or by visiting the following URL: www.cdeducation.org/password . This URL will be included in the e-mail reminder sent to you before the expiration date of your password and is also listed on the webmail page and the web page for teachers (see **Section II**). **This is the ONLY valid URL for changing your password – do not divulge your password to any other web site asking for it!**

Please note: Account passwords must never be shared with others. Sharing your password with another person is a violation of the acceptable use policy governing the proper use of the Office of Catholic Schools computing resources. Account holders are responsible for all activities conducted with their ID. Accounts that are shared will be deleted by the system administrators.

2) Privacy

The privacy of your e-mail is protected to varying degrees, depending on the method you use to retrieve your e-mail. The chart below will summarize the level of privacy offered by each of the connect methods in their default configuration:

Method of connection	Level of security (default configuration, Windows)	Notes
Pine via SSH	High	No record of your e-mail is retained on the computer you use to log in, as long as you log completely out of the system when you are done.
Webmail via Firefox/Netscape	High	No record of your e-mail is retained on the computer you use to log in, as long as you close your browser after you log out.
Webmail via Internet Explorer	Low	A copy of every message you view is saved in the "Temporary Internet Files" folder on your hard drive. No password is needed to view these files.
		IE may offer to "remember" your password for future use.
IMAP client program	Medium	Messages may or may not be copied to your hard drive, depending on the program you use. If they are, then no password is needed to view these files.
		Passwords may be "remembered" for automatic logon.
		Network traffic is not encrypted.
POP3 client program	Low	Messages are copied to your hard drive. No password is needed to view these files.
		Passwords may be "remembered" for automatic logon.
		Network traffic is not encrypted.

Computers that are shared by a number of people, such as lounge or lab computers, should never be configured to download any e-mail to the hard drive!

3) Spam

"Spam" has become a large problem for many users of the internet. The term "spam" refers to unsolicited bulk e-mail, usually of a commercial nature. The diocesan e-mail system screens all incoming e-mail and rejects any message that appears to come from a known spam source or appears to have spam content. Some messages may be passed with "[SPAM]" added to the subject line. This indicates that the message might be spam but the filter could not determine this for certain and so did not block it outright.

If you receive spam, you can report it so that messages with similar content can be filtered in the future. To do so, select the message click the button or link near the top of the webmail screen labeled "Report as Spam." There is also a "Report as NOT Spam" button/link you can use to report mislabeled "[SPAM]" or to ensure messages from mailing lists you have signed up for are not marked as spam. Please note that although some mailing lists encourage you to add their address to your address book to prevent them being blocked as spam, doing so will not have any effect under our e-mail system. The recommended way to ensure you receive your messages is to report two or three samples as "NOT Spam" to teach the filter about them.

You can also choose to reject or accept mail from specific problem addresses by creating a custom mail filter. Select option "S" from the main menu (accessible only via SSH) to edit your custom mail filter. Instructions on how to create a custom filter are provided on-screen when option "S" is selected from the main menu.

4) Viruses

Computer viruses are a significant threat to the security of any machine on a network. Viruses are malicious programs that attempt to replicate themselves using a variety of means. In addition to replicating themselves, most viruses contain a "payload" which may cause a number of undesirable things to happen to a host computer. Some viruses cause computers to freeze, while others erase hard drives. The more sinister ones are able to steal passwords or grant complete access to the computer from another location. A computer infected with this type of virus could potentially provide an intruder with full, unrestricted access to a user's files and e-mail without their knowledge, regardless of the method and care used when connecting to the network.

Therefore, it is imperative that networked computers be constantly monitored by a reputable anti-virus software package, and that software package must be updated regularly so it can keep up with new viruses as they are discovered.

One of the preferred methods of replication for many newer viruses is replication via e-mail attachments. The chart below summarizes the respective vulnerabilities of each of the methods that may be used to connect to the Office of Catholic Schools' e-mail server:

Method of connection	Level of protection from contracting new viruses (default configuration, Windows)	Notes
Pine via SSH	High	Viruses cannot be transmitted to your computer via this connection.
Webmail via Firefox/Netscape	Medium	There is no known method by which viruses may be transmitted to your computer automatically via this connection. New bugs may be discovered and exploited later, however.
		You can still contract a virus if you explicitly click on an attachment you have received, and the attachment is infected.
Webmail via Internet Explorer	Low	There are several bugs in the standard installation of IE which may allow viruses to be automatically transmitted to your computer.
		You can also contract a virus if you explicitly click on an attachment you have received, and the attachment is infected.
POP3/IMAP client program	Medium/Low, depending on program	Some e-mail programs may be tricked into automatically loading infected attachments, especially default installations of Outlook/Outlook Express.
		Many viruses use these programs to replicate themselves via the network.

The diocesan e-mail server scans all incoming e-mail attachments for viruses, so you can be reasonably certain that attachments received through this system are virus-free. However, care should still be taken when dealing with unexpected attachments since new, unidentified

viruses may slip through the scanner. In particular, files ending with the **.vbs**, **.exe**, and **.pif** extensions should be regarded with extreme suspicion.

If your computer happens to become infected with a virus, and you use a POP3 or IMAP client program, be aware the virus may try to use this program to replicate itself to other computers via the e-mail network.

II. World Wide Web Services

The web site of the Diocese of Columbus Office of Catholic Schools (www.cdeducation.org) serves two purposes. First, it provides information about the diocesan schools to the public. Second, it provides special information and resources to administrators, teachers, and staff within the school system.

A) Public information

Most of the information that is available to the public can be found by clicking on the “information” or “schools” links on the home page.

B) Resources for teachers and staff

Pages that contain special resources for teachers and faculty, such as the Fee Waiver request form, can be found at the following address: www.cdeducation.org/teachers . The latest version of this resource guide may also be found at this address.

III. Appendices

A) Appendix A: Steps for Configuring Secure Shell (SSH) for Windows

- 1) Download the latest non-commercial version of SSH from this site: **ftp.ssh.com/pub/ssh**
As of this writing, the filename of the latest version is
SSHSecureShellClient-3.2.9.exe
- 2) Install the software. You may accept all installation defaults.
- 3) Launch the Secure Shell Client.
- 4) Go to the Edit menu and select Settings...
- 5) Under "Connection," enter **cdeducation.org** for the host name.
- 6) Adjust any other settings according to your own preferences, such as Color and Font.
- 7) Click OK when done.
- 8) Go to the File menu and select Save Settings.
- 9) You may now log in to Clarus by pressing Enter.

B) Appendix B: Steps for Configuring MacSSH for Macintosh

- 1) Download the latest version of MacSSH from this site:
pro.wanadoo.fr/chombier/MacSSH/SSH_down.html
As of this writing, the filename of the latest version is
MacSSHPPC.sit
- 2) Install the software.
- 3) Launch MacSSH.
- 4) Go to the Favorites menu and select Edit Favorites...
- 5) Select <Default> and click Edit.
- 6) Enter **cdeducation.org** for the host name.
- 7) Click OK. Click OK again to close the Favorites window.
- 8) You may now log in to Clarus by selecting Open Connection... from the File menu.