

Archdiocesan Network

New User Training

10/1/2014

Archdiocese of Chicago

Mike Riley

VIDEO TUTORIALS AVAILABLE

Almost 100,000 video tutorials are available from VTC. The available tutorials include Windows 7, GroupWise 8 and Office 2010 applications.

To access these tutorials, visit <http://links.archchicago.org> and click the link for VTC Online Training. Login with your GroupWise username and password. You MUST use our custom login page from the list of Archdiocesan Web Links. You will NOT be able to login directly at VTC.com.

Once logged into the VTC site, you can view any of the available tutorials (the Flash versions tend to load that fastest). You can view as many tutorials as you want.

We have a limit of 5 concurrent users (only 5 people from our network can be logged in at one time). If all of the “seats” are currently in use, you will receive an error message.

You can also access these tutorials from home. Simply use the link provided at <http://links.archchicago.org>.

CONTENTS

IT Assistance Line.....	1
Logging In.....	2
Screen Saver	4
End of the Day	4
Rebooting	4
Logging Off.....	4
Shut Down (Hard)	5
Automatic Reboots	5
Passwords	6
Password Requirements	6
Software and Hardware.....	7
Additional Software and Hardware	7
Packaged Software	7
Office 2010 File Formats.....	7
Saving Files.....	8
Network Drives	8
My Documents Folder	8
Novell iFolder.....	8
Deleting Files	10
Restoring Files.....	11
Recovering Network Files	11
Remote Control	11
Anti-Virus.....	12
Internet Content Filter.....	13

Archdiocesan Links	14
Employee Directory	14
IT Website	14
VTC Online Training	14
Supported Internet Services	15
Training	15
Classroom Training	15
Online Training	15
E-Mail	16
E-Mail Filter	16
Whitelist/Blacklist	17
Attachments and Message Size	17
Bulk E-Mail	18
Schools	18
Others	18
Batch Mail	18
Quigley/Meyer Conference Rooms	18
Network/Internet Access	18

ARCHDIOCESAN NETWORK

IT ASSISTANCE LINE

The Information Technology Assistance Line is here to help you in technology related issues. Hours of operation are Monday through Friday, 9:00 – 4:45. In the event that no one is available or you call after hours, please leave a message on our answering machine.

IT Assistance Line: (312) 534-5227

The IT Assistance Line deals with software issues, hardware (computer) issues, network issues, login issues, purchasing (computer software and hardware), typewriter maintenance and telephone issues for the 534 exchange.

You should always call the IT Assistance Line for any issues you are encountering. DO NOT call a technician directly or send your request for assistance via e-mail. Doing so will only delay resolving your issues.

LOGGING IN

Before you can use a computer in the Pastoral Center's network, you will need to log in. When you start a computer running Windows 7, one of the first screens you will see is the log in screen.

To log into the computer:

- Hold down the **Ctrl** and **Alt** keys and tap the **Delete** key
- Click **OK** after reading the security notice to continue the login.
- Enter your network *Password* (passwords are case sensitive)
- Click **OK** or tap the **Enter** key

If you enter the wrong password when you log in, you will receive a Login Message indicating that you could not log on. You will then need to enter your Password again. However, if you enter the wrong password three (3) times within a 24-hour period, your account will lock and you won't be able to log on for one hour OR until a Network Administrator unlocks your account.



If you are NOT the last person who logged into that computer, you'll need to click on Switch User and Other User to specify your username.

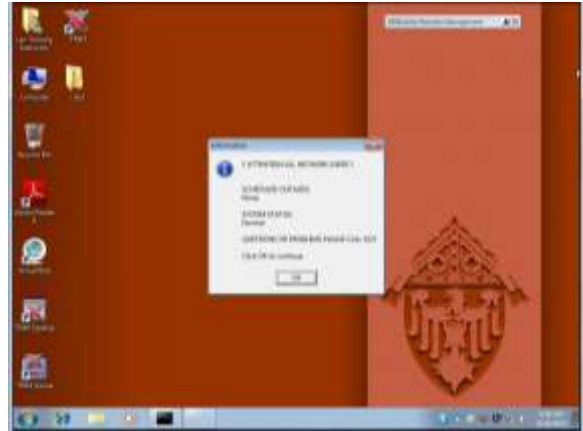


After you log into the Pastoral Center network, several things will happen:

- A login script runs and connects you to several network drives.
- Daily Update appears. You will need to close Daily Update after you read it to continue the login process.
- A network status message will appear. Click OK to continue the login process.
- GroupWise launches and prompts you for your password.
- You might be prompted to enter your Password for iFolder.



Daily Update



Network Information



GroupWise Login



iFolder Login

Each user who connects to the Pastoral Center's network needs his/her own account. Logging on as another user or allowing another person to use your User Name and Password is a violation of Archdiocesan Policy.

SCREEN SAVER

Computers within the Pastoral Center's network will also use a password-protected screen-saver which will activate after 30-minutes of inactivity. When the screen-saver activates, it will lock the user's workstation to prevent unauthorized access to the network.

To deactivate the screen-saver and return to normal use, simply move the mouse or tap a key on the keyboard. You will then need to log back into the network with your username and password.

Note: You won't be able to change the screen saver settings.

END OF THE DAY

At the end of the day, you should leave your computer turned on. There are times when we need to install updates to the software on your computer that could take several hours. In some locations, we can remotely turn on a computer...but not all locations.

If you turn your computer OFF at night and we do need to install a long update, you may have to wait several hours the next day before you can use your computer.

You should, however, log off OR restart at the end of the day (see below).

REBOOTING

If you start having problems with your computer that you weren't having before, one of the first steps in troubleshooting is to reboot (restart) your computer. This also logs you off from our network.

To reboot your computer:

- Click the Windows *Start* button
- Click the arrow to the *right* of Shut Down
- Click Restart



LOGGING OFF

You can also simply log off of the Archdiocesan network *without* restarting your computer.

To log off:

- Click the Windows *Start* button
- Click the arrow to the *right* of Shut Down
- Click Log Off

SHUT DOWN (HARD)

If your computer becomes completely unresponsive, you will need to do a “hard” shut down. To force the computer to power off, hold in the power button on the computer (not the monitor) until the computer turns off. In the event this doesn’t work, unplug the computer from the power outlet.

If you initiate a hard shut down, wait approximately four (4) seconds after the computer turns off before you turn it on again.

AUTOMATIC REBOOTS

Your computer will automatically reboot overnight. This is necessary in case any software updates will only install when you log in and to ensure that you are notified when your network password is due to expire. Make sure you have SAVED any open files before you leave or else you will lose your work.

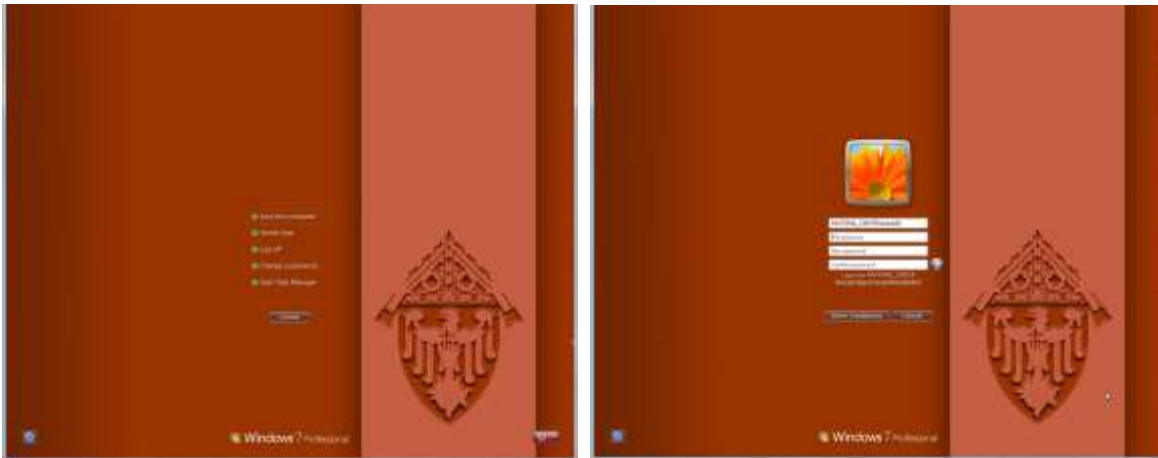
PASSWORDS

You will need to change your Pastoral Center network password every 30 days. You will begin receiving prompts that your password is due to expire 5 days before your password expires.

Your password will expire exactly 30 days from when you last changed your password—down to the exact second. If you haven't changed your password by the time you are notified that your password will expire in one (1) day, change your password immediately. As soon as your password expires, your account will lock and you won't be able to access most network resources (printers and shared drives).

To change your password:

- While logged in, hold down Ctrl and Alt and tap the Delete key
- Click on Change a password
- Enter your *current* password in the Enter password field
- Enter a *new* password in the New password field
- Enter the new password again in the Confirm password field
- Click the arrow to the right of Confirm password to make these changes



You can change your password whenever you want. You do NOT need to wait the full 30 days.

PASSWORD REQUIREMENTS

When creating a password, you need to follow a couple of rules:

- Your password must be at least seven (7) characters but no more than 13
- You cannot reuse a password for at least 13 months

When you create a password, it's a good idea to use a combination of letters, numbers and symbols. This helps prevent others from guessing what your password is. Passwords are case-sensitive. If you create your password with capital letters, you need to enter it with the capital letters when you log in.

SOFTWARE AND HARDWARE

The software that you need to use for your job should be automatically installed on your computer. Standard applications for users in our network include:

Acrobat Reader	Microsoft Access	Microsoft Word
Command Anti-Virus	Microsoft Excel	Novell GroupWise
Internet Explorer	Microsoft PowerPoint	Novell iFolder
	Microsoft Publisher	

Other applications may be available depending on the software you use in your job.

ADDITIONAL SOFTWARE AND HARDWARE

Software and Hardware installed on an Archdiocesan computer *must* be acquired through the Office of Information Technology. Software/hardware acquired through other means will NOT be installed on Archdiocesan computers.

If you feel you need additional software/hardware, contact the IT Assistance Line at (312) 534-5227.

PACKAGED SOFTWARE

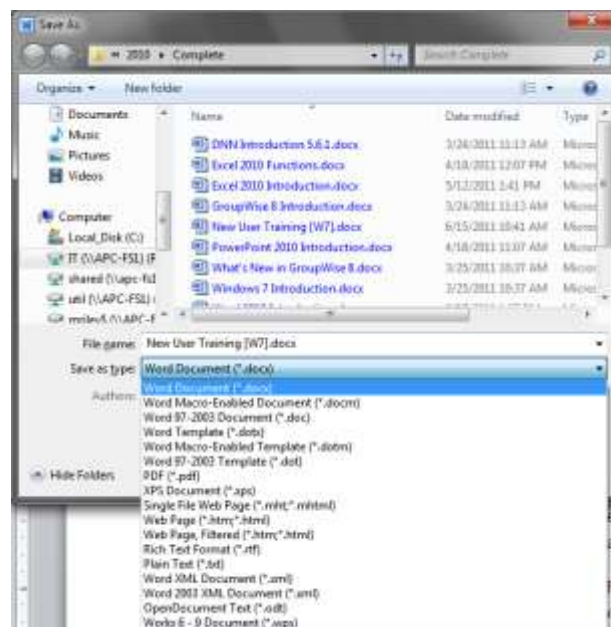
Some programs and software updates will be installed for you automatically via the Zen Application Launcher. These products will be installed without requiring any action on your part.

OFFICE 2010 FILE FORMATS

Beginning with Office 2007, the file types for Office files changed. Files saved in the newer formats can't be opened with older versions of Microsoft Office (2003 and earlier) without additional software.

Within our network, the default save format is the Office 97-2003 compatible format. This lets you share the file with the widest possible audience. However, not all of the newest features in Office 2010 will be available when the file is saved in Compatibility Mode.

You can manually save a file in the newest format using the Save As command. Choose the Save as type that is listed first.



SAVING FILES

It's important to save your work in a location that is backed up. If your computer crashes, the IT Department can only recover files that we have backups for.

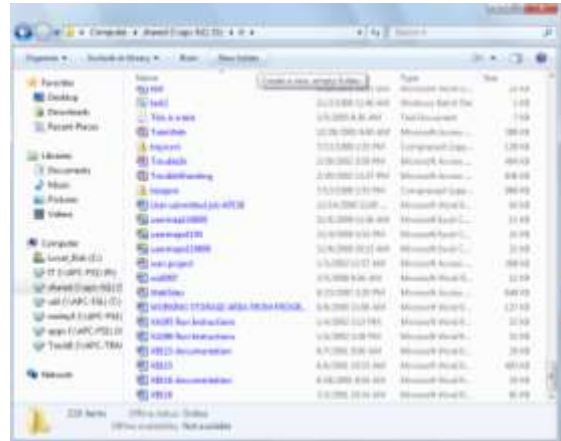
NETWORK DRIVES

The best place to save your files is on a network drive. In the Archdiocesan Network, this is typically somewhere in the R or S Drives. Some folders are available to all network users, while others are restricted to specific users.

You *may* be able to create subfolders in S:/R: drive folders if you have sufficient permissions.

To create a subfolder:

- Open the folder you are creating the subfolder within
- Click New Folder
- Type a unique name for the new folder and tap the Enter key



MY DOCUMENTS FOLDER

Another option is to save files within your My Documents folder. This folder is the default location in Microsoft products. Files you save to this folder are backed up IF you are logging into Novell iFolder.

We normally create iFolder accounts for permanent employees ONLY. If you are a temporary or volunteer employee, you should save your files in the S: or R: drive.

NOVELL IFOLDER

Novell iFolder is a utility that creates backups of files saved in your My Documents folder.

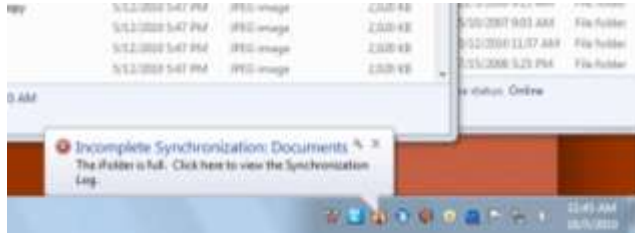
A few minutes after you log into your computer, the iFolder Login box will appear. Enter your network password and click Log In to continue.



Choosing "Remember password on this computer" will log you in automatically. When you change your network password, iFolder will inform you of the invalid (old) password and lets you enter your new password.

IFOLDER LIMITS

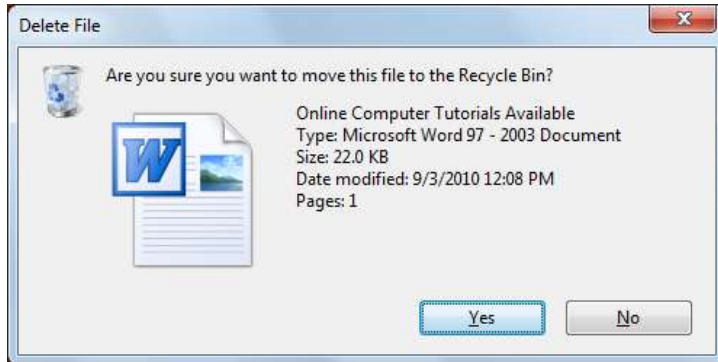
Your iFolder has a maximum capacity of 300 MB. If you exceed this limit, iFolder can no longer back up your files. You will then need to DELETE files in your My Documents folder (or move them to a different location).



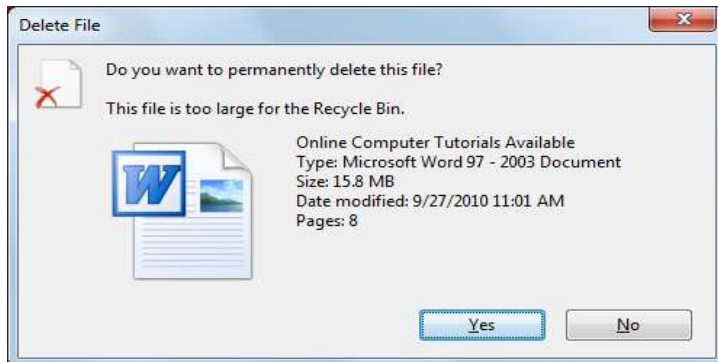
iFolder will notify you *once* per login if you've exceeded your allowed space.

DELETING FILES

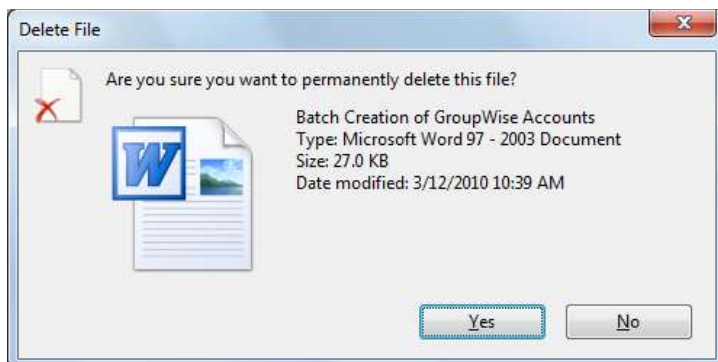
When you delete a file from your hard drive, it will normally be moved into the Recycle Bin (and remain there until you restore or empty it).



If the file is too large for the Recycle Bin, you will be prompted a *second* time.



When deleting a file from *any other location* (network drive, flash drive, etc), the file will NOT be moved into the Recycle Bin.

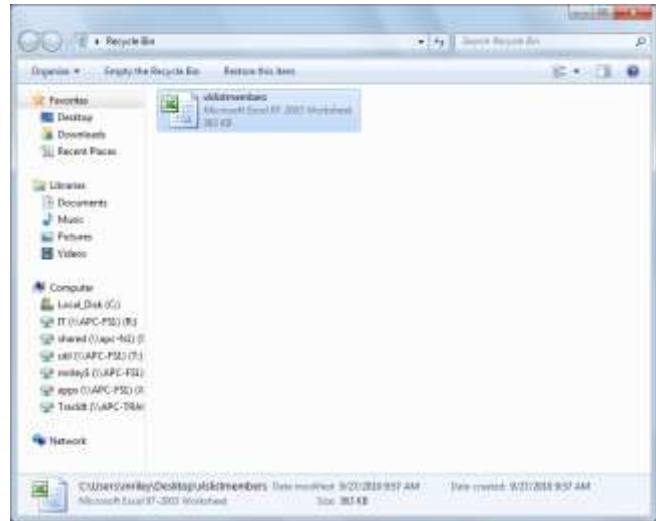


RESTORING FILES

You can easily restore files that are in your Recycle Bin.

To restore a file:

- Open your Recycle Bin
- Select the file
- Click Restore This Item
The file will be moved back to its original location



Remember, the only files that go into your Recycle Bin are files from your local hard drive (C: drive).

RECOVERING NETWORK FILES

If you delete a file off a network drive (S: or R:), please call the IT Assistance Line at 312-534-5227. If there is a backup of the file, we should be able to restore the file.

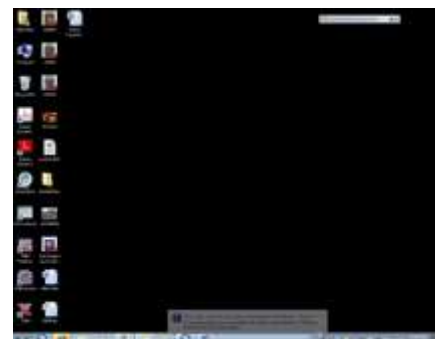
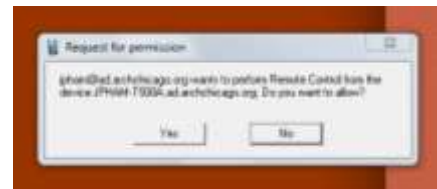
Recovering a file from backup can take up to 2 business days.

REMOTE CONTROL

When receiving assistance from Information Technology, rather than visiting you in-person to resolve your issue(s), we will likely use Remote Control utilities.

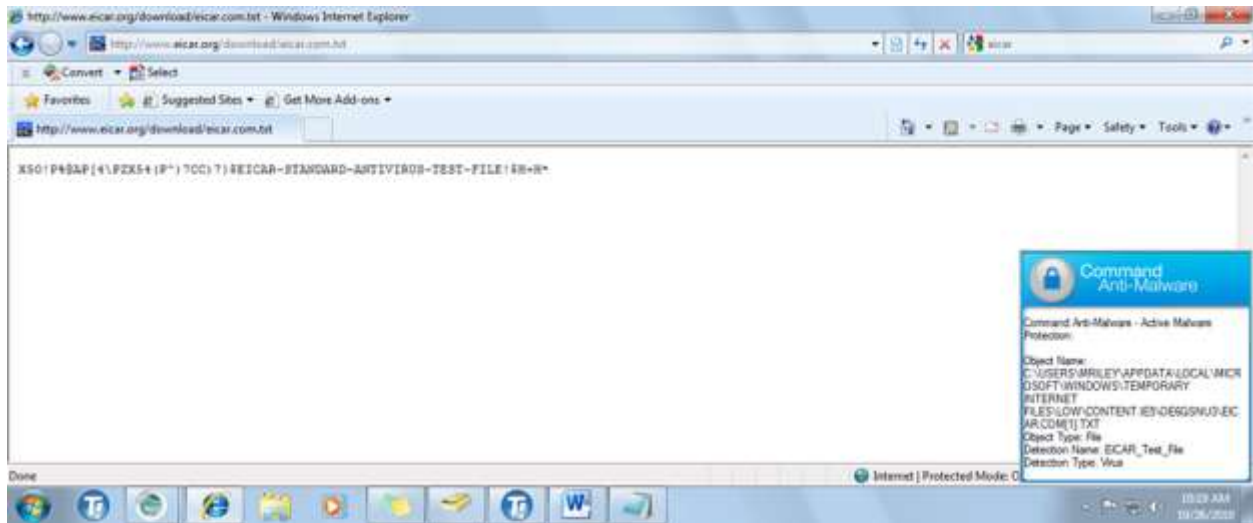
When a technician attempts to remote into your computer, you'll receive a prompt on your screen. Click Yes to allow the technician to access your computer.

While the technician is accessing your computer, your desktop wallpaper be replaced by a blank screen.



ANTI-VIRUS

Malware, malicious software, is an ongoing problem with computers and networks. To minimize the risk to our network, all computers on the Archdiocesan computer network run the Command Anti-Malware product.



If you receive an alert from Command Anti-Malware, please call the IT Assistance Line IMMEDIATELY (312 534-5227).

INTERNET CONTENT FILTER

Internet Access is requested along with the request for your user account.

Web surfing runs through a proxy server. All surfing is logged and some sites are restricted.

If you try to access a restricted site, you will be presented with a login screen similar to the one below. This informs you that the site (or page) you are trying to access is blocked. If you feel the site is blocked by mistake, please call the IT Assistance Line (312-534-5227) and open a work order to request the site be unblocked.



ARCHDIOCESAN LINKS

The Archdiocesan Links page is a listing of commonly used websites within our organization. Listed websites are public (available to anyone in the world), private (available only from within our network), or authenticated (available to anyone with an Archdiocesan GroupWise account).

You can access the links page via the Start Menu or by browsing to <http://links.archchicago.org>.

EMPLOYEE DIRECTORY

The Archdiocesan Employee Directory is available from computers within our network via the Archdiocesan Links page or by navigating to <http://emp.archchicago.org> (which redirects you to the Employee Directory).

You can search for active and former employees on this page. If you are an actual employee (not a temp or volunteer), you can also update your phone numbers that is listed by clicking Change My Work Phone. (The ability to update your work phone becomes available approximately two days after you attend New User Training.)

IT WEBSITE

The Office of Information Technology website (<http://it.archchicago.org>) is also listed on Archdiocesan Links. The IT website includes the Training page where you can register for classes and download courseware and information about synching smartphones with GroupWise.

VTC ONLINE TRAINING

VTC is an online video tutorial website that we have subscribed to. To access the VTC website, you MUST use the custom login page that we have created. This page is listed on Archdiocesan Links and the Online Training tab of the IT website.

Use the Flash format when viewing the VTC tutorials.

SUPPORTED INTERNET SERVICES

The Internet is more than just web browsing and e-mail. It is a collection of services that transfer information using a variety of methods and applications.

Within our network, we support *standard* web browsing and our GroupWise e-mail system. Other internet utilities might not work reliably within our network, if they work at all.

Web sites that use non-standard ports to transfer information will NOT work within our network.

You should always test a specific utility within our network as soon as possible before committing to using that utility. For example, most web conferencing applications provide tests that you can run to make sure they work correctly. Waiting until 5 minutes before the conference to test is NOT appropriate.

TRAINING

The Office of Information Technology has two options available for training: classroom and online training.

CLASSROOM TRAINING

Several classes are offered each month in the IT Training Room at Quigley. You can view (and register for) upcoming classes on the Training page on the IT website (<http://it.archchicago.org>) and also download courseware. Classes are on a first come/first served basis and are available to ALL Archdiocesan employees, temps and volunteers (including those work are working with parishes and schools).

If a class has open seats, simply click the Register link below the class, fill out the information and click Complete Registration.

ONLINE TRAINING

IT has also subscribed to an online training site, VTC. The VTC tutorials are available to users who have attended New User Training. To access these tutorials, you MUST access the site using our custom login page.

To access the VTC tutorials, click the Online Training link on the IT website. You will then login with your network username and password.

Once on the VTC site, you can use the Find a tutorial search box to locate the available tutorials. When choosing the media type, you should choose Flash (since they'll load faster).

We can only have 5 users logged in at one time. If you are #6, you will receive an error message on VTC.com.

E-MAIL

E-Mail is one of the most widely-used communication methods in the world. Almost every user in our network has a personal e-mail account they can use in their day-to-day work.

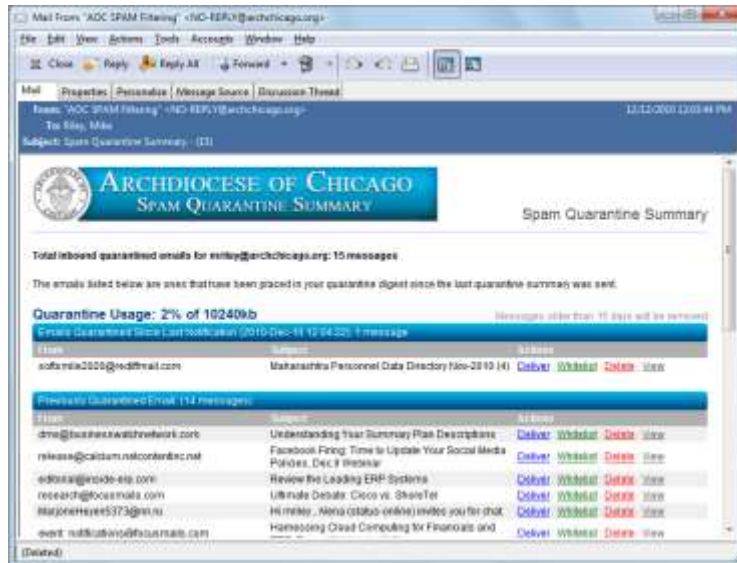
Keep in mind that e-mail isn't secure. You shouldn't e-mail confidential information to someone. As a rule of thumb, if you wouldn't fax the information, don't e-mail it.

E-MAIL FILTER

Over 90% of the messages attempted to be sent to our mail system are junk mail. To reduce the impact of junk e-mail, external inbound e-mail runs through the Barracuda e-mail filter. Messages are then either discarded, quarantined, flagged as spam, or delivered normally.

If you have any items in your spam quarantine, you will receive an e-mail from AOC SPAM Filtering. The message displays the items in your quarantine at the time the message was delivered. You can easily access your quarantine from the *most recent* quarantine notification. In GroupWise, choose View, HTML (if necessary) to view the formatted notification message.

Make sure you have already logged into the web filter (that day) before you attempt to manage your quarantine.



If you have problems accessing your quarantine from an e-mail message or want to adjust your quarantine *without* using an e-mail message, browse to <http://smtp-spam.archchicago.org> and login with your username and password.

From the Spam filtering website, you can deliver, whitelist and delete messages. You can also manage your own Whitelist and Blacklist.

WHITELIST/BLACKLIST

You can prevent an address (or e-mail domain) from being considered as spam by adding that address (domain) to your whitelist. You can also completely block senders (domains).

Simply enter the address (or domain) in the allowed or blocked section and click Add. Senders in your whitelist could still be blocked due to viruses, message size, or attachment type.

The screenshot displays the 'Spam Quarantine Summary' page for the Archdiocese of Chicago. At the top, there are navigation tabs for 'Quarantine', 'Block', and 'Preferences'. The user is identified as 'mriley@archchicago.org'. The main content area is divided into two sections: 'Allowed Email Addresses and Domains (Whitelist)' and 'Blocked Email Addresses and Domains (Blacklist)'. The whitelist section contains a table with 15 rows, each listing an email address and a domain, with an 'Add' button next to each. The blacklist section contains a table with 2 rows, each listing a domain with an 'Add' button. A note on the right side of the whitelist section states: 'Email sent from addresses entered here will not be analyzed for spam, but will be scanned for viruses.' A similar note is present for the blacklist section.

Email Address	Sub List
Clasapah3@aol.com	1
E.kron@usenet.net	1
HwanA@imgac.com	1
Jflagy@iTechDesigns.com	1
bounce.e.groupon.com	1
liron@gngold.net	1
edronew@stlarchchicago.org	1
eddwel@comcast.net	1
edwardwillerson@gmail.com	1
imgac.com	1
info@messageandflects.com	1
scytamon@yahoo.com	1
fp.org	1
mghtand@yahoo.com	1
newsletter@brainstormic.com	1
stepanuh@comcast.net	1
stefan.culmann@gmail.com	1

Email Address	Sub List
chrishop.com	1
pop-media.com	1

You should NOT whitelist a public mail system such as gmail.com, aol.com, yahoo.com, etc. Blocking an address that is actual spam is normally ineffective, since spammers tend to spoof the sending address or use different addresses each time they send messages.

ATTACHMENTS AND MESSAGE SIZE

Several types of files are blocked from coming into our post office. These files are ones that can execute code and are most often simply viruses. If someone attempts to send you a blocked file, *they* will receive an e-mail response indicating that the file type is NOT allowed.

In addition, messages exceeding 7 MB (the size of the message PLUS all attached file) will be rejected. Again, the sender will receive a response indicating that the message can't be delivered.

If someone wants to get a large file to you, or a blocked attachment, they will need to deliver it to you *without* using e-mail. This may involve them posting the file on a website or sending you a CD/DVD.

BULK E-MAIL

Our mail system contains over 3500 mailboxes. While it is *possible* to send a message to everyone in our address book, there are specific procedures you should follow.

SCHOOLS

If you want to send something to all schools and/or principals, you should send the message to Maria Ippolito in the Office of Catholic Schools.

OTHERS

If you want to send something to all parishes, priests, employees, etc (anything other than schools), send the message to Diana Kozojed in the Moderator of the Curia's office.

BATCH MAIL

Every Thursday, an e-mail is sent to all parishes. This e-mail includes content submitted from several agencies. If you want to send something to Batch Mail, simply send it to batchmail (no spaces) from your GroupWise account. The content will be reviewed and sent when approved.

Files sent in Batch Mail should be PDF files whenever possible. In Office 2010, simply use File, Save As and choose PDF as the file type.

QUIGLEY/MEYER CONFERENCE ROOMS

Conference rooms at the Quigley and Meyer centers can be reserved using GroupWise. The instructions for booking conference rooms are included in the GroupWise 8 Introduction and GroupWise 8 – Conference Rooms courseware (available on the Training page at <http://it.archchicago.org>). If you are unable to book a room on your own, the receptionists at Meyer and Quigley can book the room for you.

NETWORK/INTERNET ACCESS

Wired and wireless network access is available in all conference rooms for laptops configured for the Archdiocesan computer network. You can connect your Archdiocesan laptop to the network jack in the conference room and log into the Pastoral Center network in the same way you log in at your desk. Wi-Fi network access is available via the AOC-SECURE Network.

Visitors who are giving presentations in the conference room and need Internet access can log into the AOC-GUEST Network. Login information is available from the receptionist at Quigley and Meyer. If you will need guest access on the weekend, you will need to request the login information on the workday prior to the weekend.

Archdiocesan employees can access the internet with *personal* devices using the AOC-LUNCH network available in the lunch rooms at both locations. Login information is posted in each lunch room.

Direct any questions or comments to the IT Assistance Line at (312) 534-5227.

APPENDIX

Removing blasé AutoCorrect Entry in Microsoft Office

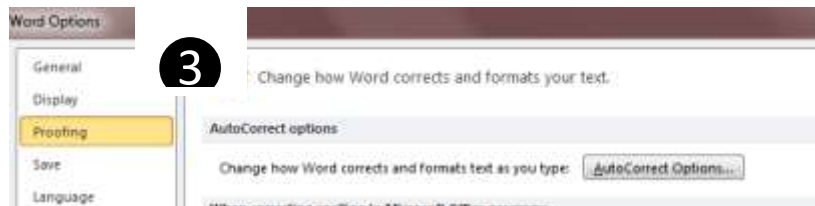
In Microsoft Office, the autocorrect feature corrects commonly misspelled words and adds accented characters for some words. One such word that is autocorrected is blasé.

Of course, this is going to pose a problem if you are typing Archbishop-Designate Cupich's first name (Blase).

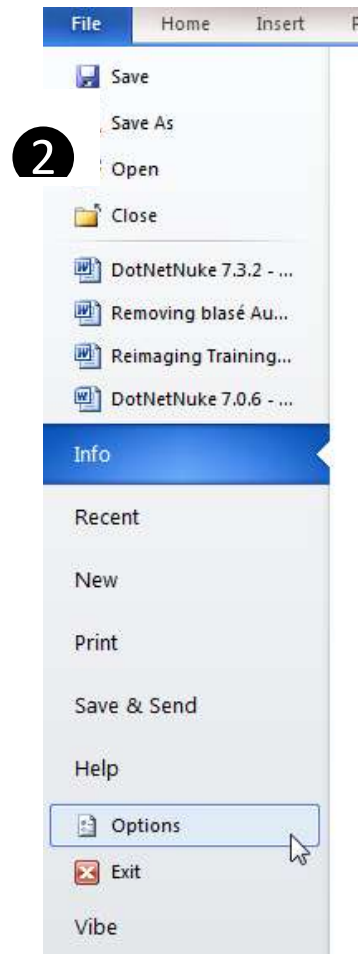
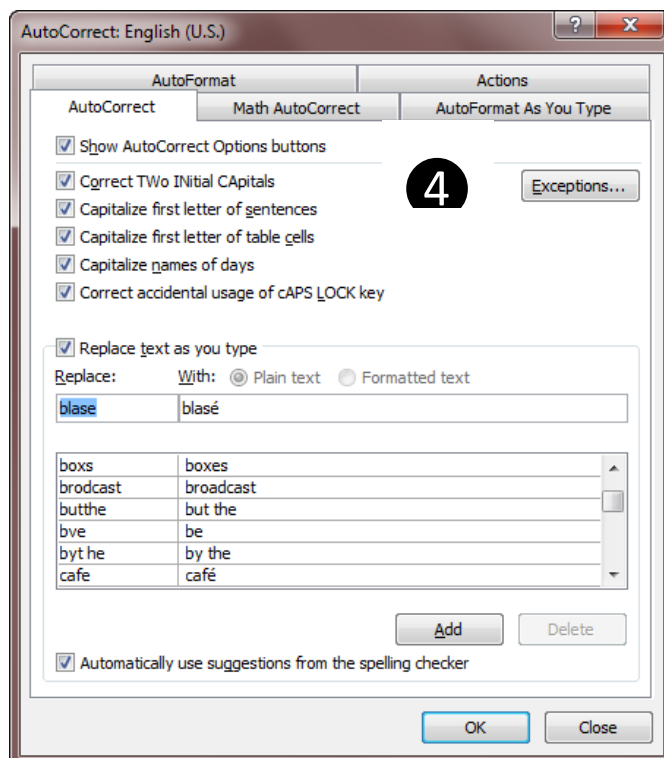
You will want to REMOVE this entry from your AutoCorrect options to prevent this from being automatically changed in Microsoft Office applications (Word, Excel, PowerPoint, Access, Publisher).

To remove the entry:

1. Start Microsoft Word
2. Choose File, Options
3. Select Proofing and click AutoCorrect Options.



4. In the Replace: box, start typing the word "blase" to jump to its entry. Select it from the list of options and click the Delete button. Click OK as



needed to close the options.

Note: If you switch computers, are upgraded, or reimaged, you will need to make this change again.

We are unable to push this change to all users without removing any user-created AutoCorrect options.