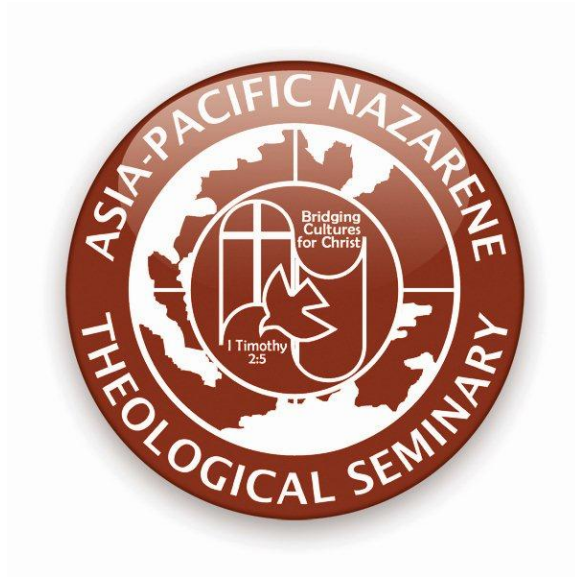


Technology Handbook



Asia-Pacific Nazarene Theological Seminary

1st Semester, 2011-2012

Table of Contents

Chapter One: Introduction	1
Chapter Two: Basic Computer Operation	3
Chapter Three: Network Access	6
Chapter Four: Using Moodle	8
Chapter Five: Email	11
Chapter Six: Virus Protection	15
Chapter Seven: Seminary Web Site	23
Chapter Eight: Maintenance	25
Chapter Nine: Contacts	28

Chapter One

Introduction

Computers are wonderful tools to aid in ministry and education and have become indispensable for communication and information.

The computer technology at APNTS is provided for learning, teaching, communication, community building, and administrative purposes consistent with the seminary's mission and vision. The goal in providing these resources is to promote educational excellence in ministry preparation by facilitating resource sharing, innovation, and communication. The use of this technology is a privilege, not a right. Access entails responsibility. All technology accessing the network should be used in a responsible, legal, and ethical manner.

This handbook is an attempt to inform the seminary community about the use of the computer network and systems on campus. Effort has been made to provide as many answers as possible in a short space. When a question arises, students, staff and faculty should first consult this handbook, and when there are still lingering questions, should contact the appropriate person listed in the appendix.

Philosophy of Technology Use


Technology is a means to an end and not an end in itself. It is one more tool to use to complete the job to which God has called us. As a tool, it can be used in beneficial ways but also in ways that can be harmful. With the aid of new technology also comes responsibility. There are many wonderful resources on the Internet that cannot be found anywhere else. At the same time, with access to computers and people all over the world comes the potential availability of material that may not be considered of educational value in the context of a seminary setting. There are many sites that are inappropriate for Christians to view, and many are contrary to the Gospel of Jesus Christ.

Proper behavior, as it relates to the use of computers, is no different than proper behavior in all other aspects of the seminary. All conduct at the seminary should be governed by the imperative to be holy like God is holy. Any activity that violates the call to be holy and biblical standards of holiness should be avoided. The model of the New

Testament church living in an unholy society should be carefully considered.

Resources Available

The seminary is constantly trying to improve its technology resources. These resources have increased in significant ways over the past few years. We need to be good stewards of our blessings. As of the writing of this handbook, the available resources include the following:

- Computers for student use in the library.
 - Internet access in the library, dining hall, and dormitories
 - Software that is adequate for research and writing
 - Access to the library catalog through the Internet (<http://www.apnts.edu.ph/library>)
 - Network folders for students
 - Access to online course resources through the Moodle program and EBSCOHOST
 - An email account for each student
 - 25GB online storage using the APNTS email account (<http://skydrive.live.com>)
 - Links on the library website to resources for research
 - Printing capability in the library
- 

Chapter Two

Basic Computer Operation

Operating computers can be very challenging, and at times frustrating, especially with the sophistication of modern operating systems. Students are encouraged to become familiar with their computer operating system and the programs they use most. When in doubt, always check the “Help” menus for the various programs. The best guide is experience and learning what to do and not to do. The following are some brief suggestions for basic computer operation.

Power

Computers contain sensitive electronic components and are vulnerable to electrical surges. Therefore, everyone is encouraged to use surge protectors for their computers. These are available at nearby hardware stores (make sure the power strip is actually protecting from electrical surges and is not simply an extension cord). When a computer is not being used for long periods of time or if there is a bad storm coming (which often happens here), you should unplug it. Surge protectors do not always protect from direct lightning strikes. Computers also consume electricity and should not be kept on except during ongoing work or for certain office computers. If you come from another country, be sure to check the voltage of your computer. The Philippines uses 220 volts and most outlets on campus are 220 volts. There are a few outlets that are 110 volts. These should be clearly marked.

Hardware

Become familiar with your computer: the power buttons, reset button, output and input ports like the USB, printer, video, mouse, keyboard, network, modem, FireWire, and others. Consult your owner’s manual to familiarize yourself with the functions of your computer. Do not take your computer case apart unless you know what you are doing. Static electricity can harm sensitive components.

Software

There are thousands of programs available, and it is difficult to learn how they all work. Some software is copyrighted and needs a license to operate. As Christians, we ought to be mindful about using illegal copies of software, even though they are easily available in the local market places. There is a lot of free software available for public use

that can do just about anything licensed software can do. The seminary uses Microsoft Windows XP on many of its systems through a licensing agreement with Northwest Nazarene University. This software may not be put on personal computers not owned by the seminary. If your computer does not have a good operating system, the APNTS IT department can make copies of Ubuntu for you for a small fee. It will be your responsibility to install this operating system yourself.

Basic Principles for Using Computer Software

- When in doubt, use “Help.” When “Help” doesn’t help, check the Internet.
- Understand menu bars and icons. Know the layout of the program.
- Always double check your work before you print (spell and grammar check).
- Always test your slide show before you show to the public.
- Always proofread your email before you send it.

Word Processing Suggestions

- Check all formatting requirements for your specific project, including page number, margins, fonts and font sizes, and general layout.
- Know how to save in different formats and how to open documents in different formats (the “Save” and “Save as” options).
- Familiarize yourself with how to edit a document with copy, paste, and delete.
- Understand how to insert various enhancements into your document, including photos, graphs, and various graphics.
- Using footnotes and endnotes are very important in a research institution. Know how to do this.
- Understand how your program formats a page and page contents.

Suggested Word Processing Programs:

- Microsoft Word: Used by most people; licensed
- Corel Word Perfect: Powerful for large documents; licensed
- OpenOffice Writer: Almost equivalent to Microsoft Word but free of charge
- Star Office: Similar to OpenOffice, both free and licensed versions

Note: When you send a document to a person to read, be sure the person can open the file. Common formats include .rtf (rich text format) or OpenDocument format. Most modern word processing programs are compatible, but beware that MS Word has problems reading certain formats.

Do's and Don'ts of Slide Shows

- Keep your audience in mind. Don't make the show too busy so that it distracts from your presentation.
- Be professional in the slide show itself and in your personal appearance.
- Do not be locked into your slide show or your notes. Your object is to communicate your ideas.
- Check your equipment before you show. Practice running the equipment. You cannot interrupt your presentation to fiddle with the equipment. Run your slide show on the equipment to make sure it works.
- Make the slide text big enough for the audience to see comfortably. Rule of thumb: 1 inch of view screen for each person: for 100 people, you should have a 100 inch view area; for 1000 people have a 1000 inch view area.
- If used in conjunction with other people or events (for example, in a church setting), be sure to coordinate the slides with the presenters.

Suggested Slide Show Programs:

- Microsoft PowerPoint: Powerful and comprehensive, but is licensed
- Corel Presentations: Similar to PowerPoint; licensed
- OpenOffice Impress: Does mostly what the above do but is free.

General Comments about Computer Use:

- § Leave equipment in good working order after using it. Keep the work area clean for the next person.
- § Do not alter (called "hacking") or delete files or data on any seminary computers.
- § Do not install software or hardware on seminary computers.
- § Do not disconnect any cables or dismantle any computers. Some computers will not run if they are not connected to the network.

Following these simple guidelines will enable everyone on campus to make effective use of our technology.



Chapter Three

Network Access

Accounts

All registered students will be given an account name and password to access email and Moodle. Account logins and passwords will be provided the first week of each semester to registered students. They will remain in effect until the close of registration the following semester.

Web filtering

The campus network filters web sites and content considered inappropriate. This system is not perfect and is highly configurable. If you are trying to access a web site but are blocked by the filter, please send a note to the APNTS network administrator for evaluation and adjustment of the filter program.

Facebook Fasting

Facebook will be blocked on Wednesdays. To encourage the campus community to realize the time and the dangers being spent on social networking, we encourage students, faculty and staff to “fast” from Facebook each Wednesday, and spend more time in prayer, meditation, and study, and, especially, to maximize other forms of face-to-face interpersonal fellowship.

Limiting downloads

Downloading large files such as music, video, or programs slows down the network for everyone else, and may be illegal if the program is copyrighted. The student network is setup to limit the amount, speed, and types of download. Again, if you find this prohibiting your research, send an email to the network administrator to consider modifying the filter system.

Internet Connections

Students may access the Internet in the following locations:

1. Library: wired and wireless
2. Computer Laboratory
3. NCEE Palm Tree wireless
4. Dorm rooms: wired
5. Owen’s Hall wireless

Students are responsible for obtaining their own network cable which can be purchased at nearby computer retailers or in the I.T office. Students may not access the internet through the wired ports in classrooms reserved for teaching.

Connecting personal computers to the network

You may connect your personal computer to the student network by following these directions:

1. Wired connections: Personal computers may be connected at the places listed above. Students will need to adjust their personal computers to access the seminary network following these directions:

No Network configuration is needed: You may set your configuration to automatically detect an IP address from the server. For most computers, this means all you need to do is plug in your computer's network connection to the campus network. Nothing more needs to be done here. **Do not set an IP address for your computer because it may lead to system conflicts.**

2. Public wireless access points are available at the locations listed above. You will need to search for available networks and then connect to the one that says "APNTS Public" (NCEE Palm Tree). Set your Internet connection to automatically receive an IP address as described above.

Please Note: All personal computers connected to the seminary network must have an anti-virus program (see Chapter Six on viruses).

Printing

Students may print from the computers in the Computer Laboratory. They are connected to the network printer/copier in the circulation area. The cost for printing will be given by the Librarian. The library provides the paper. Any other printing will need to be done on personally owned printers.

A general suggestion: Plan ahead and make sure your printer is ready to print your assignments. Extensions may not always be given just because "My printer ran out of ink." For printer installation, please see the manual for your specific printer. Most problems occur because of improper driver installation or empty ink cartridges.

Chapter Four

Using Moodle

The seminary is using an open source classroom program called *Moodle* (<http://www.moodle.org>). Moodle is being used by thousands of schools all over the world. It can be used for both on-campus and distance education courses. All students should become familiar with the basic operation of this program.

Accessing Moodle

The APNTS Moodle web site is called “Learn Online” and is available on the Internet at <http://learn.apnts.edu.ph>. You may also link to this from the seminary’s main web site: <http://www.apnts.org>.

Some parts of the Moodle web site are available to the general public (certain discussion forums). Other parts are available only to faculty and registered students. All registered students will be given an account name and password to access Moodle.

The following are basic instructions for accessing Moodle. More in depth directions can be found on the Learn Online website given above. Look on the left column of the web site under the “**Main Menu**” for the menu item called “**How to use Moodle.**”

Logging In

The login screen is located on the upper right column of the Moodle home page. You will need to supply the correct user name and password. There are several additional options there for logging in: Creating a new account, Forgotten password, and Guest login. Please do not create a new account. It will be deleted by the Moodle Administrator.

Enrolling in a Course

Upon logging in, the courses for which a student has registered will show up in the left column labeled “**My Courses.**” Just click on the course title and you will be taken to the course web page.

If you have not been enrolled in a course (a separate process than enrolling for courses in the registrar’s office), you may self-enroll if you have the course enrollment key which is supplied by the professor of

the course. If this is the case, then click on the appropriate semester under “**Course Categories**” on the left column of the Moodle home page. Then find the course you will be enrolling in. After clicking on it, you will be prompted for the course key. After entering the correct key provided by your instructor, you will have access to the course. You only need to enroll once for each course.

Changing Password or Updating Profile

You have the option of setting your own password or updating your personal profile. To access this, click on your name at the top of any page once you have logged in. This will take you to your personal page. On this page there are several options, including editing your profile or sending a message to another user. Check your profile to make sure it is accurate (name, address, email, phone). You may not change your account name. Do not change anything you are unsure of. You can also upload a picture if you would like one attached to your name. To add a picture, you must first have a picture saved on your local computer or on a disk/flash drive, etc.

- Click the **Browse** button on the right side of the “New Picture” text box to open the Choose File dialog box.
- Locate your picture on your computer.
- Select the picture file
- Click the **Open** button

When finished, scroll down and click the **Update Profile** button at the bottom of the page. A page should display saying “Changes Saved.” Click the **Continue** button to go back to your Profile and see the additions and changes you made.

Accessing Course Materials

After logging in, you may access the courses in which you are enrolled. Each course layout will be slightly different, depending on how the instructor has set it up. Moodle makes it easy to access various materials—just follow the links and menu items. Generally, here are some items to be aware of:

1. Accessing Course Material:

Teachers may post different kinds of material on the course web site. The most common will be documents and slide shows. Most of the time, these will be in Microsoft Word and PowerPoint formats or in PDF format. If your computer does not have these products, other programs will also open them, especially OpenOffice. You may also

- Download free viewers from Microsoft for all MS Office products: <http://www.microsoft.com/office/000/viewers.asp>

- Download the free Adobe Acrobat Reader at <http://www.adobe.com>.
- Download OpenOffice free office program that allows one to view MS Office produces: <http://www.openoffice.org>.

Please Note: Certain browsers, like Internet Explorer, will block you from downloading files. You need to click on the access denial bar at the top of the browser to allow the file to be downloaded.

1. **Joining Discussion Forums:** After choosing this item, you may post responses or begin new threads.
2. **Uploading Assignments:** If your teacher has assigned a project to be uploaded, simply click on the assignment on the course home page. One of the options will be to upload a file. Any time you upload a file in Moodle and push the “Browse” option, it will go to your local computer. Here, you will need to find the location of the file on your local computer. After uploading the file to the Moodle server, the teacher will be able to read it. The teacher may give you the option of updating the assignment until the due date. Please be aware: Moodle will say if the assignment is late.
3. **Viewing Grades:** Teachers have the option of posting the grades on line. If so, you will be able to access these from the course home page. Sometimes professors will use MS Word’s comment feature to provide feedback on your assignments. They will then upload the graded assignment onto Moodle for you to view. You should receive an email notifying you that your graded assignment is available for download on Moodle. By clicking on the link provided in the email, you may download the graded paper, open the file, and view the comments. If the comments are not visible, select “Markup” from the View menu (MS Word) to reveal the comments. If you have difficulty viewing your professor’s comments, please ask for assistance.

Greek and Hebrew Keyboards

In the Learn Moodle home page, you can find a PDF link on **Unicode for Greek and Hebrew**. There you see instructions on installing Greek and Hebrew keyboards, you are encouraged to use these keyboards, unless directed otherwise by your instructor.

Email

General Guidelines

Email has become one of the most used communications tools in modern history. We are happy to provide each student his or her own email account as part of the registration process. Email accounts are created and managed by the Network Administrator. Email accounts are provided to students upon enrollment. The seminary will provide students lifetime email accounts.

As email becomes more available to the campus community, the following points should be kept in mind:

- § Users should not post chain letters or engage in “spamming.” Spamming is sending unsolicited messages to a large number of people, or sending a large number of unsolicited messages to one or a few individuals.
- § All users should check their email frequently and delete unneeded messages off the server to save storage space.
- § Users should subscribe only to high quality discussion groups or mail lists that are relevant to their education and career development.
- § Incoming mail that is misaddressed will remain undeliverable. Please be certain to give out the correct email address.
- § There is the potential that files attached to email messages may contain viruses, therefore, all users are encouraged to be cautious about opening messages with unknown contents or from unknown people. Especially avoid opening any file with .exe@ or a program executable file. Any such messages should be immediately deleted without saving or opening the attachment. The most common way for computer viruses to be spread is through email.

Practice Basic “Netiquette”

- § Respond to email messages as soon as possible, preferably within 24 hours. If you cannot give a full response, at least acknowledge the receipt of the letter and that you will respond more fully at another time.
- § Use language that is considered appropriate for Christians. Be both professional and personable in your communication.
- § Send information that other users will not find offensive.

- § Maintain confidentiality in all communication.
- § Post or forward others' personal communications only with the original author's consent.
- § Use *asterisks* around words to emphasize them.
- § Use *emoticons* or smileys when making a joke in order to let others know that what is being said is actually a joke: :-) :-(.
- § Use normal case when typing. Using all capital letters is often referred to as *shouting* on the Internet.
- § Be careful about sending sensitive information (financial or personal records) in an email, because there are no *private* messages on the Internet.
- § Proofread any messages for spelling and grammatical errors before sending.
- § Use the Golden Rule and treat others with the same respect as if you were talking face-to-face.
- § Use a signature line at the end of your messages and include your name, position, favorite quote or other important description of you or your work.

Accessing Your Email

There are several ways to access APNTS email.

1. Webmail

Go to this web address: <https://mail.apnts.edu.ph/>

Enter: *username@apnts.edu.ph*

Enter: *password*

After this, you may read your mail, compose, delete, forward, and other useful mail options.

2. Personal Computer

It is assumed that your computer has access to the Internet. If you need help accessing the Internet on campus, please see Chapter 3.

Email Programs

1. Outlook

- ⇒ Tools
- ⇒ Email Accounts
- ⇒ Add a new e-mail account
 - Choose "POP3"
- ⇒ Click "Next" button

Add the following information on this page:

➤ Your Name: *Your real name*

➤ E-mail address: *username@apnts.edu.ph*

- User name: *username@apnts.edu.ph*
- Password: *your password*
- Check “Remember Password”
- Incoming mail server: *pod51003.outlook.com*
- Outgoing mail server: *pod51003.outlook.com*
- ⇒ Click “More Settings . . .”
- ⇒ Click “Outgoing Server” tab
 - Check “My outgoing server (SMTP) requires authentication”
- ⇒ Click “Advanced” tab
 - Check “This server requires an encrypted connection (SSL)”
 - Put in the box next to “Incoming server (POP3)” this number: 995.
 - Check “This server requires an encrypted connection (TLS)”
 - Put in the box next to “Outgoing server (SMTP)” this number: 587.
- ⇒ Click “OK”
- ⇒ Click “Finish”

Note: Outlook Express will be slightly different, but use the same settings as above.

2. **Mozilla Thunderbird**

- ⇒ Edit
- ⇒ Account Settings...
- ⇒ Click “Add Account” button
- ⇒ Check “Email Account”
- ⇒ Click “Next”
 - Your Name: *Real Name*
 - Email Address: *username@apnts.edu.ph*
- ⇒ Click “Next”
 - Click “POP”
 - Incoming Server: *pod51003.outlook.com*
- ⇒ Click “Next”
 - Incoming User Name: *username@apnts.edu.ph*
- ⇒ Click “Next”
 - Account Name: *Anything You Want to Name Your Mail Settings*
- ⇒ Click “Next”
- ⇒ Click “Finish”
- ⇒ On left column, click “Server Settings”
 - Server Name: *pod51003.outlook.com*

- Port: 995
 - User Name: *username@apnts.edu.ph*
 - Under “Security Settings” check “SSL”
-
- ⇒ On left column, click “Outgoing Server (SMTP)”
 - Click the name in the white box and choose “Edit”
 - Check “TLS”. Make sure the port reads 587.
 - ⇒ Click “OK” twice.

Note: APNTS email uses a secure connection.

Mailbox limit

Mailbox size is 10GB.

Online Storage

SkyDrive (<http://skydrive.live.com>) has 25GB of online storage space.

SkyDrive is a service that comes with your APNTS email address that would allow you to create, edit, and share Microsoft Word, Excel, and PowerPoint files online—even if you don’t have Microsoft Office installed in your computer. Share photos and videos with anyone you choose—including your social network. You can control the permissions of those who can view your files.

Changing e-Mail Password

To change your password just logon to your APNTS Live@edu email account and choose *Options*. It will direct you to the Options page and change your password from there.

Chapter Six

Virus Protection

Viruses are here to stay—at least for the foreseeable future. The severity, sophistication, and magnitude of attacks have increased dramatically. ALL computers connected to the APNTS network in ANY way must have virus protection.

Users of a personal computer are responsible to ensure that their computers are virus-free and well protected, by taking the following actions:

- educate yourself about virus protection
- use all functions of anti-virus software
- keep computer operating system updated
- keep anti-virus software installed and current
- develop safe e-mail habits
- avoid harmful or suspicious applications

Computer users who suspect their computer has a virus should immediately disconnect from the network, then disinfect the computer and protect against further attack.

To recover from a virus attack and subsequent blockage from the network, users have two options: 1) request disinfection assistance from the IT department, or, 2) disinfect the computer on their own or with other outside help.

About Viruses

None of us likes to devote much time or thought to the subject of computer viruses. Many choose to ignore the problem—hoping that their computer will not be a victim. In today's computing environment, that is no longer an option. The sad truth is, destructive viruses are more prevalent, more dangerous, faster spreading, and harder to counteract than ever before, and they are not going away. Most likely you have already had to deal with one or more attacks on your computer—or you soon will.

APNTS is doing all they can to protect our network, but it is the **RESPONSIBILITY OF EACH COMPUTER OWNER** to ensure that his or her computer is adequately protected and is not spreading viruses to others on campus.

What are Computer Viruses?

There are three main types of computer virus:

- A **true virus** can hide itself in a variety of mediums: applications, boot sectors, etc. Some viruses operate as macros within other files, such as Word documents. When an infected file is opened from a computer connected to APNTS network, the virus can spread throughout the network and may cause damage.
- A **Trojan horse** is an actual program file that, once executed, can damage the computer on which the file was run.
- A **worm** is also a program file that, when executed, can both spread throughout a network and do damage to the computer from which it was run.

NOTES:

About virus hoaxes. Many well meaning people are fooled into spreading virus hoaxes. Do not pass along virus scares or glibly follow instructions unless you are CERTAIN it is not a hoax. If you suspect a virus hoax, you can research the topic at several reputable websites, such as this one: <http://hoaxbusters.ciac.org/>.

Intentionally spreading viruses is a crime. APNTS will cooperate fully with the authorities, and will not shield users of our network who engage in illegal behavior.

How do Viruses get on my Computer?

Viruses can enter your computer and APNTS network in a variety of ways:

- **E-mail** — Many viruses are sent out as e-mail attachments. While our email server tries to block viruses from entering our campus email system, it is impossible to block all of them. These attachments could be working documents or spreadsheets, or they could be merely viruses disguised as pictures, jokes, etc. The attempt to spread a virus may be intentional or completely unintentional. The sender may not even know the message or attachment has been sent. Once some e-mail viruses are opened, they look for e-mail addresses or distribution lists and automatically e-mail themselves. The sender may not know his or her computer is infected and is spreading the infection.
- **Files or software downloaded from the Internet** — Downloading via the Internet is a major source of infection. As with other types of transmissions, the virus could hide within what appears to be a legitimate document, spreadsheet, or other type of file, such as a music file. This happens frequently in peer-to-peer “file sharing”

environments, such as KaZaa, Morpheus, IMesh, BearShare, Bittorrent, and Grokster.

- **Floppy Disk, USB drive, CD, Zip disk, or other storage media** — As with e-mail attachments, the virus could hide within a legitimate document or spreadsheet or simply be disguised as another type of file.
- **Instant messaging** —Virus and worm creators are setting their sights on IM services, such as Microsoft Instant Messenger, Yahoo Instant Messenger, ICQ, etc. Typically the attack comes in the form of a false message, many times from a KNOWN sender.
- **Direct attack** — via the Internet or a network connection. This is an area that is also on the increase. Virus writers or perpetrators are sometimes able to make use of security weaknesses to launch direct attacks on other computers. The only defense, short of total isolation, is to follow proven anti-virus practices (see below).

How can I Protect My Computer from Virus Attack?

Educate Yourself

There is an abundance of information easily available to anyone with an Internet connection. The various computer magazines, such as PC-World (<http://www.pcworld.com>), PC Magazine (<http://www.pcmag.com>) and many others have very informative web sites. There are numerous governmental and anti-virus software vendor sites that are very useful. For example, the United States Department of Homeland Security sponsors a site at Carnegie Mellon Software Engineering Institute, <http://www.cert.org>

Useful anti-virus maker web sites include Symantec, makers of Norton anti-virus (<http://securityresponse.symantec.com>), McAfee anti-virus (<http://us.mcafee.com>), and Kaspersky anti-virus (<http://www.kaspersky.com>).

Keep Anti-virus Software Installed and Current

For whatever their dark purposes, virus writers seem to be very busy people. New strains and entirely new viruses are unleashed continuously. Because of this, anti-virus software companies are constantly updating their “definition files”—the tools that identify and protect against known viruses. In some anti-virus applications, it is not obvious when the license has expired, and the updates are no longer being downloaded. For example, many new computers come with a short subscription, some as short as 90 days. Just having the anti-virus

software installed does not protect you! The subscription must be current and the virus definition files up-to-date.

Use all the Functions of the Anti-virus Software

Most good anti-virus software can be configured to automatically update the virus definitions, to automatically monitor all computer activity, including all incoming files, and to automatically do periodic “full system scans” of your computer. Learn to use these functions and keep up on their status.

NOTE: You should also consider installing **personal firewalls** such as free version of zone alarm. Although the IT Department maintains a firewall for all traffic entering and leaving the campus, a personal firewall can protect your computer from unauthorized access from inside the campus, such as the intrusive activity of many viruses.

Keep your Computer’s Operating System Up-to-date

Microsoft is constantly releasing patches and updates to Windows, Internet Explorer and other Windows components. Make use of the free and simple automatic update feature built in to all Microsoft operating systems since Windows 98.

Develop Safe E-mail Habits

- DO NOT generally open attachments. Only open attachments when:
 - you know who the person is
 - you know exactly what the attachment is, and
 - you are expecting it.
- If you know the sender but are not sure, ask the sender if the attachment you received was legitimate. They can always re-send it. In other words, **don’t be quick to click!**

Avoid Harmful or Suspicious Applications

Peer-to-peer (P2P) file-sharing programs, such as KaZaa, Morpheus, iMesh, BearShare, and Grokster pose serious network security threats and could lead to legal entanglements. All have been identified as known carriers of a variety of spy-ware applications. Some of this spy-ware attempts to steal personal information, including Social Security numbers, credit card information, etc.

Freeware and shareware programs abound on the Internet. Only download these applications from well-known, reputable sites.

Instant Messaging applications can also cause problems. If you really want to use IM, try to settle on one IM program and stick to it. Installing every IM program on the planet is an unnecessary security risk.

APNTS Virus Policy

Required Protection

1. All computers connected in any way to the APNTS network are **REQUIRED** to have up-to-date, active, anti-virus protection.
2. It is the computer owner's responsibility to ensure, at a minimum, the following safe computing practices are followed:
 - a. Virus definitions are up-to-date (never more than one week old).
 - b. The anti-virus software is configured to actively monitor all inbound and outbound data.
 - c. Exercise extreme caution when opening attachments. Never open an attachment unless it is expected—even if it is from a trusted sender.

Note the distinction between **receiving** an e-mail message that contains a virus-laden attachment versus **opening** an attachment and allowing a virus to infect a computer. Most active computer users receive many e-mail messages that contain viruses. By knowing the proper way to dispose of these messages, users can prevent any harm from coming to the system (see the Computing Resources section of the APNTS Intranet for help).

- d. Exercise extreme caution when downloading files from the Internet.
- e. Make sure your virus protection is completely up-to-date before installing new software.

Three Anti-virus Solutions

There are a huge number of antivirus solutions available today. Following are just three examples as suggested choices for APNTS students.

Good: AVG - Free Antivirus Software on the Web

INDIVIDUAL users can download a free version of GRI Soft AVG Antivirus. Note that the licensing rules **CLEARLY** state that AVG Anti-Virus FREE Edition is available for single home computer use only. It is

not intended for computers that are used to conduct the business of an institution, such as APNTS office computers.

Also please be aware that, according to independent testing, AVG does NOT PROVIDE AS GOOD OF PROTECTION as other antivirus applications, such as Kaspersky or Norton (see below). However, if it is all you can afford, it is MUCH BETTER THAN NO PROTECTION.

To download a free version of AVG, browse to <http://free.grisoft.com/freeweb.php>

Better: Kaspersky Antivirus (KAV)

Kaspersky Antivirus is a relative newcomer to the field, but they have rapidly built a reputation for providing top quality virus protection. In independent tests, KAV consistently earns very high marks.

Best: Norton Antivirus

“Best” is always a debatable term, but Norton consistently wins the highest marks for antivirus protection, ease of use, etc. It is a very solid program. However it is also one of the more expensive applications on the market. Current yearly subscription rates (Norton 360) are about US \$69.99 (or **P3009.57**).

Norton Antivirus can be purchased in stores or online here: <http://www.symantec.com>

Virus Diagnostic Check-up Service

If the user is not certain that their computer is adequately protected, or if they need assistance installing an anti-virus application, they can leave their computer in the Central Office, IT room for a checkup. Updating of virus definitions will be free but if the virus has caused damage to the computer and reformatting is needed, the student will be charged **P100/hr** for system configuration, student will provide installers of the operating system and necessary drivers.

Payment is made in the Accounting Office. Check-ups and anti-virus installations will be performed on a first-come, first-served basis. The service may take several days to complete.

The following services are included in the diagnostic check-up:

1. Check for existence and up-to-date subscription of anti-virus software.
2. If antivirus software is already installed, but the subscription is expired, give the student the option of paying for a new subscription installing a free application such as AVG or supplying their own software for installation.
3. Configure anti-virus protection appropriately so that it monitors the computer all the time, keeps itself updated, and generates some sort of reports when virus activity is suspected.
4. Perform a full scan of the system to ensure it is currently virus free. If it is found to have viruses see step number 3 under “In Case of Virus Infection” below.
5. Check for and apply any critical operating system updates.
6. Instruct the user in sound protection practices, including:
 - a. proper use of the anti-virus software
 - b. what to do in case of infection
 - c. importance of and how to perform system updates
7. When the technician is satisfied that the computer is protected, its identifying information will be recorded.

In Case of Virus Infection

1. If a user detects a computer virus, the first step should be to **IMMEDIATELY DISCONNECT** from the network (including physically unplugging the network cable). This is to prevent spreading of the virus to others, and to prevent network access from being blocked by the IT Department.
2. If the user does not disconnect and the IT department detects virus-like activity, **the offending computer’s access to the network may be disabled by IT staff.**
3. To recover from a virus attack and subsequent blockage from the network, the user has **two options**:
 - a. **request disinfection assistance** from the IT department, or
 - b. **disinfect the computer on their own** or with other outside help

Disinfection Service Provided by APNTS

Assistance of the IT team for disinfecting computers is OPTIONAL. If the user requests assistance, fees will be charged. See chapter 8.

Disinfection Process without IT Help

Of course, users are free to choose to disinfect the computer either on their own or with other outside help. The following steps, **at a minimum**, should be taken.

1. Check the Internet for the latest virus alerts and updates.
2. Follow the instructions to disinfect the virus, and to ensure your computer is well-protected from future attack.
3. If your computer has been blocked from access to the APNTS network, bring the following information to the IT Manager:
 - a) Your computer's full "computer name" and your network adapter's machine address (or physical address [also known as MAC]).

Getting your computer's physical address:


- (a) Go to **Start | Run**
 - (b) Type **cmd** in the **Run** command window to launch the command prompt
 - (c) In the command prompt, type **ipconfig /all**
 - (d) Copy the *physical address* that was returned by the previous command
- b) A scan report (attachment) from your antivirus software that shows the virus has been successfully removed.

IMPORTANT: Make sure your anti-virus software has a **current subscription** and the virus **definitions are up-to-date**.

Negligence

The following conditions are defined as negligence, in regard to adequate virus protection practices. If any of these conditions are found to be the case, fees for assistance will be increased.

- Failure to keep a currently licensed up-to-date and activated anti-virus software application installed on the computer (virus definitions not more than one month old).

- Installation or use of a known, high-risk peer-to-peer file sharing application such as, but not limited to: KaZaa, Morpheus, IMesh, BearShare, and Grokster.
- 

Chapter Seven:


Seminary Web Site

The seminary has been building a web site that contains useful information for students, staff, faculty, alumni, potential students, and friends. The seminary community is encouraged to make regular use of the web site. The web site can be found at:

<http://www.apnts.edu.ph>

The following are the main contents of our web site:

1. Home page:
 - Quick links and navigation bar to the rest of the site
 - Get the latest news and find out about upcoming events
2. About
 - Mission and Vision
 - History
 - Statement of belief
 - Giving and Volunteer Opportunities
3. Academics
 - Faculty
 - Programs of Study
 - Owens School of World Mission
 - Accelerated English Program
 - Academic Policies
 - Guides to Research Writing
 - Instructional Policies
 - Course Descriptions
 - Accreditation and Validation
 - Library
 - Course Schedules
 - On-line Class Resources
4. News
 - Recent News
 - Events Calendar
 - The Bridge Newsletter
5. Admissions
 - Applying to study at APNTS
 - International students
 - Fees

- Financial Assistance
 - Housing
 - Student Testimonials
 - Contact Registrar
6. Alumni
- Alumni News
 - Alumni Directory
 - Alumni Officers
 - Update Information
7. Community Life
- Student Body Organization
 - Chapel Service recordings
 - Student Handbook
 - Upcoming Events
 - Directory
 - Link to Webmail
8. Resources
- Ministry Resource Center
 - Mediator
 - Discussion Board
9. Contacts
- Contact directory
 - Links
- 

Chapter Eight

Maintenance and Security

Personal Computers

The APNTS IT staff is responsible for up keeping all seminary owned computers. Individuals are responsible for the upkeep of their own personal computers. Under no circumstances is the IT staff responsible for the maintenance of personal computers. The IT staff will only assist students, staff, or faculty with personal computer problems if time allows. If there are other institutional technology needs, they will take priority.

Problems with login and passwords and configuring personal computers to access the seminary network will be resolved free of charge.

The IT staff will charge the following rates for any maintenance of personal computers (billed through the Business Office):

- *Diagnostic service:*
Free.
- *Virus checkup and removal*
Free.
- *System reformatting/configuration* (student supplying the operating system)
P100.00/hr.
- *Hardware installation* (memory modules, hard drive, optical drives, etc.)
P100.00
- *Network cables*
P100.00/meter including RJ-45 connectors

All fees will be billed through the Business office.

Tutorials

The IT staff will be available as often as possible for help on basic network access and computer operation.

*****All system users should first carefully follow the directions in this handbook BEFORE consulting the IT staff.***

Seminary Owned Computers

The IT staff will do its best to maintain the computers owned by the seminary. These include those found in staff and faculty offices, library, and student computer lab.

If any seminary owned computer ceases to function properly after the user follows normal procedures of logging off and rebooting, immediately notify the IT staff because a malfunction could be signs of more serious issues.

The IT staff will assess the seriousness of the situation and may not respond immediately to all needs, depending on availability and priority.

Statement on Privacy

- § The seminary respects the privacy of the information on its networks but reserves the right to access all information on the network for safety issues (related to threats against people) or for network maintenance (an example being virus detection). The existence of passwords for folders and files on the network does not restrict or eliminate the seminary's ability or right to access information on the network.
- § Please be aware of hacking, which is breaking into files, email, and websites. Computer hackers are able to access many files through the Internet. The seminary maintains a firewall to protect the files of the network users.
- § Access to certain information and files may be restricted to protect the administrative security of the seminary and its records, and rights of privacy and confidentiality. Users who are provided access to such restricted information and files shall exercise the utmost care to prevent unauthorized persons from gaining access to such information and files, and to maintain the confidentiality of such information.

Security

- § Security on any computer system is a high priority, especially when the system involves many users. Users should immediately notify the Network Administrator if they identify a possible security problem. If any users feel that their privacy or account has been inappropriately used, he or she should immediately notify the Network Administrator.
- § Users are responsible for their own login and password and should take all reasonable precautions to prevent others from being able to use these passwords. Users should log off public computers as soon as their work or time is completed.
- § The seminary will not disclose user names or passwords at any time.
- § Users are responsible for the appropriate storage and backup of their data.
- § Data on the computers for student use is not completely secure (no technology ever is), although the IT staff will make regular backups. Users should have their own backup of important files on their own media, including floppy disks, CDs or USB drives.

Discipline for Violating Policies

- § Violation of the privacy and security policies may result in the possible loss of network privileges or, where appropriate, disciplinary action and/or counseling.
- § Users should be aware that a computer program keeps record of all network activity, and that the network is monitored on a regular basis by the Network Administrator including the web sites logged onto.

Seminary Responsibility

- § The seminary will upkeep and upgrade the computer network as much as is financially possible. The technology provided by the seminary is an as is, as available basis. The seminary does not make any warranties against system failure, loss of data, or failure of the programs on its computers. Neither does the seminary warrant that the system will be uninterrupted or error-free, nor that defects will be corrected.
- § Use of any information obtained via the Internet is at user's own risk. The seminary specifically denies any responsibility for the accuracy or quality of information obtained through its services.
- § Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not necessarily the seminary.

§ The seminary will not be responsible for any financial obligation arising through the unauthorized use of the seminary's computer resources.

Chapter Nine

Contacts

Questions will arise, so please contact the following people for help.

Process for solving problems:

- First, carefully read this handbook.
- For further questions and help, contact the IT Department at 1107.
- Otherwise, contact the responsible person.

Contact	Phone	Email
---------	-------	-------

Information Technology Office Contact: Admiral Ato	1107	aato@apnts.edu.ph
---	------	-------------------

- General questions
- Login and password problems
- Hardware problems and maintenance

Administrator: Floyd Cunningham	1103	fcunningham@apnts.edu.ph
---------------------------------	------	--------------------------

- Suggestions and questions related to overall administration

IT Manager: Admiral Ato	1107	aato@apnts.edu.ph
-------------------------	------	-------------------

- Suggestions and questions related to day to day operations

IT Technicians: Fatima Pernecita Mark Javier	1107	fpernecita@apnts.edu.ph mjavier@apnts.edu.ph
--	------	---

- Wiring problems
- Library computers
- Dining Hall computers
- Switch/Hubs

Webmaster: Arlene Fabros	1321	arlene.fabros@gmail.com
--------------------------	------	-------------------------

- Website suggestions and errors