

Acceptable Use Policy for Davis College

Introduction

Davis College provides its users with Internet access and electronic communications services as required for the performance and fulfillment of job responsibilities.

Users must understand that this access is for the purpose of increasing productivity and not for non-business activities. Users must also understand that any connection to the Internet offers an opportunity for non-authorized users to view or access corporate information. Therefore, it is important that all connections be secure, controlled, and monitored.

To this end, users in Davis College should have no expectation of privacy while using college-owned or college-leased equipment. Information passing through or stored on college equipment can and will be monitored. Users should also understand that Davis College maintains the right to monitor and review Internet use and e-mail communications sent or received by users as necessary. Davis College uses Web Inspector from Elron Software to monitor and filter web traffic.

Permitted use

The Internet connection and e-mail system of Davis College is primarily for business use. Occasional and reasonable personal use is permitted, provided that this does not interfere with the performance of work duties and responsibilities.

Users may use Davis College Internet services for personal improvement, outside of scheduled hours of work, provided that such use is consistent with professional conduct and is not for personal financial gain.

Users may send and receive e-mail attachments that do not exceed 2 MB in size, provided that all attachments are scanned before they are opened by Davis College chosen anti-virus software.

Users may send and receive short text messages with no enclosures for non-business purposes. Davis College requests that the personal e-mail not be read in the office and that any personal e-mail you receive be forwarded to a non-business account to be viewed at your leisure.

Prohibited use

Users shall not use Davis College Internet or e-mail services to view, download, save, receive, or send material related to or including:

- Offensive content of any kind, including pornographic material.
- Promoting discrimination on the basis of race, gender, national origin, age, marital status, religion, or disability.
- Threatening or violent behavior.
- Illegal activities.
- Commercial messages.
- Gambling.
- Sports, entertainment, and job information and/or sites.
- Personal financial gain.
- Forwarding e-mail chain letters.
- Spamming e-mail accounts from Davis College e-mail services or college machines.

- Material protected under copyright laws.
- Sending business-sensitive information by e-mail or over the Internet.
- Dispersing corporate data to Davis College customers or clients without authorization.
- Opening files received from the Internet without performing a virus scan.
- Tampering with your company handle in order to misrepresent yourself and the college to others.

Summary: Users are forbidden from using Davis College electronic communications systems for other charitable endeavors, private business activities, or amusement/entertainment purposes unless expressly approved by the Davis College president or his representative. Employees are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use

Responsibilities

Davis College users are responsible for:

- Honoring acceptable use policies of networks accessed through Davis College Internet and e-mail services.
- Abiding by existing federal, state, and local telecommunications and networking laws and regulations.
- Following copyright laws regarding protected commercial software or intellectual property.
- Minimizing unnecessary network traffic that may interfere with the ability of others to make effective use of Davis College network resources.
- Not overloading networks with excessive data or wasting Davis College other technical resources. This includes installing software that is ad supported.
- (In reference to a memo put out by Dr. Miller) College computers are to be used only by the people that they are assigned to. This also means family and friends are not to use the computers as they often violate the usage policies.

Violations

Violations will be reviewed on a case-by-case basis. If it is determined that a user has violated one or more of the above use regulations, that user will receive a reprimand from his or her supervisor and his or her future use will be closely monitored. If a gross violation has occurred, management will take immediate action. Such action may result in losing Internet and/or e-mail privileges, severe reprimand, or termination of employment at Davis College.

Addendum to the College's Acceptable Use Policy

Overview

As an addendum to the college's Acceptable Use Policy—which details the utilization of the college network, the Internet, e-mail, and employees' personal computers—this policy prohibits the use of Peer-to-Peer (P2P) file-sharing applications and goes into effect immediately.

The college's goal with this additional policy is to:

- Realize the maximum productivity from each employee.
- Address any potential liability from instances when employees download copyrighted material.
- Minimize network disruption.
- Protect the network from exposure to malicious code (worm, virus, Trojan horse).

- Protect the college's intellectual property.

Here is an explanation of each issue as it relates to file-sharing applications and our college:

Worker productivity

The ongoing health of the college is contingent upon each worker giving each task his or her maximum attention and effort. Using a file-sharing application to search for files, downloading them onto the college network or a client machine, and reading or playing them at a workstation is not germane to an employee's job duties and does not enhance a worker's productivity. Another issue is the possibility that P2P applications could disrupt software on an employee's workstation.

Liability

Although many materials have been placed on P2P networks with a creator's consent, much of the material (images, software, movies, music, video) has been duplicated from copyrighted materials. Downloading such files onto the college network or a client machine places the college at significant risk for legal action by the copyright holder and other organizations. File-sharing networks also provide ready access to pornography or other offensive material, subjecting the college and its employees to additional legal risk.

Network disruption

While the college has significant Internet bandwidth to accommodate all business-related activity, performance can degrade significantly when P2P file-sharing applications are used, especially when large files are being downloaded. This problem is compounded when other users on the P2P network use college bandwidth to download files from the employee's computer, which can significantly slow other services such as e-mail, Web browsing, and—more significantly—e-commerce on the college Web site.

Security

P2P networks can introduce significant gaps in an otherwise secure network. Threats such as worms and viruses can easily be introduced into the college's network. P2P applications, if modified, can also allow users outside the college to gain access to data on the employee's computer or even the corporate network. (Although most P2P applications allow users to disable file sharing, such measures do little to prevent threats from being downloaded onto a user's machine.) Some P2P applications will also allow third parties to see the user's IP address. The use of so-called spyware, which can allow network users to see your Internet browsing or can harness the use of your machine's resources, is also common on many P2P applications.

Protecting the college's intellectual property

The use of P2P file-sharing applications can sometimes allow other members of the P2P network to have access to everything on your local machine, putting the college's intellectual property assets, as well as an employee's personal information, at risk.

Virus protection policy

It is the responsibility of everyone who uses Davis College's computer network to take reasonable measures to protect that network from virus infections.

This policy outlines how various viruses can infect Davis College's network, how Davis College's IT department tries to prevent and/or minimize infections, and how Davis College's network users should respond to a virus if they suspect one has infected Davis College's network.

How viruses can infect Davis College's network

There are actually three various types of computer viruses: true viruses, Trojan horses, and worms. True viruses actually hide themselves, often as macros, within other files, such as spreadsheets or

Word documents. When an infected file is opened from a computer connected to Davis College's network, the virus can spread throughout the network and may do damage. A Trojan horse is an actual program file that, once executed, doesn't spread but 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.

Viruses can enter Davis College's network in a variety of ways:

1. **E-mail**—By far, most viruses are sent as e-mail attachments. These attachments could be working documents or spreadsheets, or they could be merely viruses disguised as pictures, jokes, etc. These attachments may have been knowingly sent by someone wanting to infect Davis College's network or by someone who does not know the attachment contains a virus. However, once some viruses are opened, they automatically e-mail themselves, and the sender may not know his or her computer is infected. Our email server has anti-virus protection installed, but there is always the chance that one will slip through. There are actually five threats to email:
 - Viruses and Worms - Viruses and worms are introduced daily; email is the main vehicle for their proliferation. New and more dangerous strains are on the horizon. One large email provider estimated a 50% increase in 2003 alone.
 - Spam - Despite the CAN-SPAM act, this is also on the increase. In a move that blurs the lines between Spam and viruses, a growing number of computers are being hijacked by spammers and used as spam distribution machines. For companies, the growing problem of unwanted email decreases their ability to conduct day-to-day business productively.
 - Malformed Messages - Malicious programmers may deliberately malformed messages to either evade virus scanners or directly attack mail server systems. Malformed messages can flood email servers leading to Denial of Service (DoS) attacks that interrupt important business communications.
 - Unauthorized Access - Illegal access to your email is a major threat to us. Encrypted email needs to be processed easily so as not to interfere with daily company business.
 - Internal policy violations - This occurs when email gets through that violates HR, IT or legal corporate policies and mandates.
2. **Disk, CD, Zip disk, or other media**—Viruses can also spread via various types of 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. For transfer from your home PC, please email the document so that our anti-virus can check it out. However, you should have up-to-date anti-virus on your own computer. Free, 100% effective antivirus software can be downloaded at www.grisoft.com. Look for the AVG Free Edition to download.
3. **Software downloaded from the Internet**—Downloading software via the Internet can also be a source of infection. As with other types of transmissions, the virus could hide within a legitimate document, spreadsheet, or other type of file.
4. **Instant messaging attachments**—Although less common than e-mail attachments, more viruses are taking advantage of instant messaging software. These attachments work the same as e-mail viruses, but they are transmitted via instant messaging software.

- 5. Peer-to-peer file sharing programs** – These programs are not allowed on our network to begin with, so usage is a violation to begin with. It is very common to have viruses spread by these programs because of the low security involved.

How Davis College's IT department prevents and/or minimizes virus infections

Davis College's IT department fights viruses in several ways:

Scanning Internet traffic—All Internet traffic coming to and going from our network must pass through college servers and other network devices. Only specific types of network traffic are allowed beyond the organization's exterior firewalls.

For example, an e-mail message that originates outside of the network must pass through the Vexeria Antivirus software before it is allowed to enter the e-mail server. This software routes suspicious e-mail and attachments to an isolated storage device, defeating the purpose of a virus.

Running server and workstation anti-virus software—All vulnerable servers run Symantec Antivirus. This software scans our file-sharing data stores, looking for suspicious code.

Symantec Antivirus Client is also installed on all organization workstations. This software scans all data written to or read from a workstation's hard drive. If it finds something suspicious, it isolates the dubious file on the computer and automatically notifies the help desk.

Routinely updating virus definitions—Every 2 days, server virus scanning programs check the Symantec update site for updated virus definitions. These definition files allow the software to detect new viruses. If a new virus definition file is available, the virus scanning software is automatically updated, and then the system administrator is informed.

When end users turn on their computers at the beginning of the workday, the workstation virus protection program checks with a Davis College server on the network for updates. The workstation program will then download and install the update automatically, if one exists.

How to respond to and report a virus

Even though all Internet traffic is scanned for viruses and all files on the college's servers are scanned, the possibility still exists that a new or well-hidden virus could find its way to an employee's workstation, and if not properly handled, it could infect Davis College's network.

The IT staff will attempt to notify all users of credible virus threats via e-mail or telephone messages. Because this notification will automatically go to everyone in the organization, **employees should not forward virus-warning messages**. On occasion, well-meaning people will distribute virus warnings that are actually virus hoaxes. These warnings are typically harmless; however, forwarding such messages unnecessarily increases network traffic.

As stated, it is the responsibility of all Davis College network users to take reasonable steps to prevent virus outbreaks. Use the guidelines below to do your part:

1. Do not open unexpected e-mail attachments, even from coworkers.
2. Never open an e-mail or instant messaging attachment from an unknown or suspicious source.

3. Never download freeware or shareware from the Internet without express permission of the IT department.
4. If a file you receive contains macros that you are unsure about, disable the macros.

Notify the help desk of suspicious files

If you receive a suspicious file or e-mail attachment, do not open it. Call Davis College's help desk at extension 404 and inform the support analyst that you have received a suspicious file. The support analyst will explain how to handle the file.

If the potentially infected file is on a disk that you have inserted into your computer, the antivirus software on your machine will ask you if you wish to scan the disk, format the disk, or eject the disk. Eject the disk and contact the help desk at extension 404. They will instruct you on how to handle the disk.

After the support analyst has neutralized the file, send a note to the person who sent/gave you the file notifying them that they sent/gave you a virus.

If the file is an infected spreadsheet or document that is of critical importance to Davis College, the IT department will attempt to scan and clean the file. The IT department, however, makes no guarantees as to whether an infected file can be totally cleaned and will not allow the infected file to be used on Davis College computers.

Virus Detection and Prevention Tips

1. **Again, Do not open** any files attached to an email from an unknown, suspicious or untrustworthy source.
2. **Do not open** any files attached to an email unless you know what it is, even if it appears to come from a dear friend or someone you know. Some viruses can replicate themselves and spread through email. Better be safe than sorry and confirm that they really sent it.

First thing to remember: **Don't be the one.**

While most if not all our computers have virus scanners that check for email viruses, one may still get through.

To make sure that you are not "the one" I suggest the following rules:

- 1) **Never open any email attachments.**

Exceptions to the rule: The three "if" test.

- **If the file is known to be on the "acceptable type" list**
- **If you know the sender**
- **If you were expecting the file**

All file attachments **MUST** pass all three "If" tests. Any files that do not pass all three get deleted.

The list of acceptable types of files includes: Word, Excel, and PowerPoint files. However, “.exe” files, for example, are not. I particularly stress the importance of the third If test. It takes only a moment to call a coworker and confirm that the message wasn't from a phantom sender. We have seen viruses come through posing as documents from someone we know, so while they may pass the first two “If” tests, it may not pass the third.

Then there is the fabled fourth “If” test: If the file you open has macros, disable them.

1. **Do not open** any files attached to an email if the subject line is questionable or unexpected. If the need to do so is there always save the file to your hard drive before doing so.
2. **Delete chain emails and junk email.** Our Spam Assassin email server usually detects SPAM and a tag is inserted into the subject line. Please do not forward or reply to any to them. These types of email are considered spam, which is unsolicited, intrusive mail that clogs up the network.
3. **Do not download** any files from strangers.
4. **Exercise caution** when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an anti-virus program checks the files on the download site. If you're uncertain, don't download the file at all or download the file to a floppy and test it with your own anti-virus software.
5. **Update your anti-virus software regularly.** Over 500 viruses are discovered each month, so you'll want to be protected. These updates should be at the least the products virus signature files. You may also need to update the product's scanning engine as well. On our computers, this is done automatically when you log on your workstation.
6. **Back up your files on a regular basis.** If a virus destroys your files, at least you can replace them with your back-up copy. You should store your backup copy in a separate location from your work files, one that is preferably not on your computer. If you do not think you have a automatic backup running, please contact Computer Services or refer to the Faculty Staff User Guide available online at www.davisny.edu/csd/guides.
7. When in doubt, **always err on the side of caution** and do not open, download, or execute any files or email attachments. Not executing is the more important of these caveats. Check with your product vendors for updates that include those for your operating system web browser, and email. One example is the security site section of Microsoft located at <http://www.microsoft.com/security>.

Do not use **Microsoft Outlook Express** as this program has low security and will allow virus-infected attachments through. Please only use Microsoft Outlook 2000.

Procedures Regarding File Confidentiality and Computer Usage Concerns

(Originally released July 1999)

One of the many changes here at Davis College is found in the Data Processing and Office Services Departments. The change is minor, consisting of a name change to reflect the evolution of duties. The Data Processing department is now the Computer Services and Information Department. This department handles all related items to computers and their usage in the office and classroom. This includes paper, diskettes, printer supplies, and computer equipment. Any changes in computer equipment must go through the Computer Services Department so that the use of this equipment is fully optimized.

With this in mind, the area of file confidentiality must be reviewed. Each person is responsible for security on his/her computer. All computers have password capability in the boot up, log-on into the Windows operating system, and finally screen savers. The accounting software we use on campus also has its own security passwords, and the server is password protected. All this is designed to keep those who do not have the right to certain information from obtaining access to those areas of personal and confidential files. People with lower access levels are not to use another's computer or account to get higher access to the information. If someone in your department needs more information, then a request must be submitted to the VP of your department. If you need to share the contents of your hard drive with another office, please password-protect the drive. If sharing is not needed, make sure that the option is removed.

With this in mind, some of the offices in our institution have the responsibility to maintain records of a confidential nature due either the nature of or by the request of the persons involved. The Computer Services Department is the primary office for keeping the data up to date and secure. So to keep and protect our employees, constituency, and our school the following procedures are and must be followed:

- 1) No Information of any kind is to be given to un-authorized persons. If there is any question at all concerning who is allowed particular information, see the VP of Business Affairs or the Computer Services Manager.
- 2) No information is to be discussed with employees or others outside of the department. If important information is to be disseminated it will be done through the appropriate channels, for example, the President's Office.
- 3) No information of a confidential nature is to be given to any student without special prior permission of the Business Office, who will then tell the Computer Services Department what information is to be released. This includes all mailing lists.
- 4) Information that is overseen by another department such as Academic Affairs, Business, administration, etc. will be accessed, disseminated and changed by, or under the direction of, that department.
- 5) The following areas are confidential files: All accounting records, all donor records and receipts, all mail, all student records, and our mailing list.
- 6) The computer in your office is assigned to you, not anybody else. Therefore the responsibility of who has access to and what on your machine is yours. Let us remember that God has been good in providing the means to get this equipment and to use it to glorify Him.

Please take care to honor the trust given us to handle honorably the information in our department.

Software Policy

Davis College computer services software installation procedure

Overview

Purpose

The purpose of this procedure is to address all issues relevant to software installation and deployment on Davis College computer systems.

Authority

This procedure has full support from the Davis College administration and business office. The Computer Services and Information Department (hereafter referred to as CSID) Director administers this procedure. This procedure is currently effective for all Davis College, employees and computer systems.

Continuance

This procedure is a living document and may be modified at any time by the CSID manager, administration, or the business office.

Software installation procedure

Mission

Davis College's CSID objective is to enable our employees to perform their tasks with technology that is in good operating condition while appropriately addressing the business needs.

Dilemma

Historically, we have not consistently addressed how software is to be deployed to Davis College's computer systems. This lack of a standard procedure has adversely affected the CSID mission at times. This procedure will set protocol as to how software is to be delivered to better enable CSID to achieve its objective of delivering stable, well-performing technology solutions.

Installation and support of Davis College software

The Davis College CSID is exclusively responsible for installing and supporting all software on college computers. This responsibility set includes:

- Office desktop computers.
- College laptop computers.
- Computer Center desktop computers.
- Telecommuter home computers (provided by the college).

The Davis College CSID relies on installation and support to provide software and hardware in good operating condition to Davis College employees so that they can best accomplish their tasks.

Current software

Davis College CSID, in coordination with all other departments, has decided upon the following software standards:

Desktop operating system

- Microsoft Windows 2000 Professional
- Microsoft Windows XP Professional

Productivity tools package

- Microsoft Office 2000 or 2003 with latest Service Packs
 - Word
 - Excel
 - PowerPoint
 - Access (Professional Edition users only)
 - Outlook 2000

Financial software

- BlackBaud's "Accounting for Non-profits" and "The Raiser's Edge."
- GradPro College Database
- Financial Aid programs (Financial Aid office only)

Internet software

- Microsoft Internet Explorer 6.0
- Microsoft FrontPage (authorized office's only)

Accessories

- WinZip (Windows XP has built-in Zip file handling)
- Adobe Acrobat Reader
- Symantec Norton Antivirus Corporate Edition
- GAIM Instant Messenger

The current software can exist in any one of the following scenarios:

- An CSID-created "image" or OEM installation on the hardware
- A Davis College CSID installation procedure that provides for the following:
 - Installation options
 - Upgrade considerations (if applicable)
 - Data conversion (if applicable)
- A shortcut to a network application (not truly an installation)
- An automated installation through an CSID-developed solution that may be used in a rapid-deployment scenario or silent-install situation
- A terminal application, Citrix application, or other thin-client type of application accessible via the Davis College intranet page

Software **cannot** be present on Davis College computers in the following scenarios:

- An installation not by a procedure
- A piece of software purchased for one's home computer
- A downloaded title from the Internet
- A pirated copy of any title
- A different title from the current software list of this procedure
- Any means not covered by the ways that software can exist on Davis College computers
- This also includes ad-supported software such as Precision Time, Date Manager, Weatherbug, and others. If a window pops up and asks to install something, please read it first to see what it is.

Software licensing

Most of the software titles on Davis College's current software list are not freeware; therefore, the cost of software is a consideration for most titles and their deployment.

It is the goal of the CSID to keep licensing accurate and up to date. To address this, the CSID department is responsible for purchasing software licenses for the following software categories:

- Desktop operating system software
- Productivity tools package
- Internet software
- Accessories

The other software categories (workgroup-specific titles) are the purchasing responsibility of the workgroup in which they serve. However, the application(s) are still installed and supported by the CSID.

To control costs, licensing costs are a factor in the decision-making processes that go into client software planning and request approval.

Software requests

If a user is to request software for their computer, the proper method will be to fill out the Davis College support request. This is simply using the Tasks in Outlook and sending it to computers@davisny.edu. The requests may also be made through the GAIM Instant Messenger program.

This is also a means to suggest additions to the current software set for Davis College. A response is guaranteed within one business day. If the Urgent option is selected or an in-person appearance occurs, a solution may be delivered at the first possible time. All in-person or "walk-in" requests are logged by a manual entry into the support request system to track licensing needs and costs.

Summary

Davis College software installation procedure

This procedure is designed to let Davis College employees achieve their business objectives. Any deviation from this strategy will require the CSID to redeploy software and/or hardware solutions. Full cooperation with this procedure is appreciated so that all goals can be met in accordance with the business objectives.