

technology

Reference

Guide



Williams College
Office for Information Technology
2008-2009

Table of Contents

Services & Resources

Faculty/Staff Support Desk: x4090	5
Student Support Desk: x3088	5
Instructional Technology Liaisons	6
Instructional Technology	7
Media Services: x2112	7
Classrooms & Computer Labs	8
Media Studios	9
Technology Training	9
Blackboard@Williams	10
Equipment Loan Center: x4091	10
Williams Students Online: WSO	11
Purchasing a Computer	12
Software	12

Quick Guides

Passwords & Accounts	13
Email	14
Viruses & Safe Computing	18
Working From Off-Campus	19
Setting up Web Pages	21
Listservs	22
Wireless	22
Data Storage on File Servers	23
Backing up Data	24
Green Computing	24
Downloading Software	25
Printing to a Network Printer	26
Computing Ethics & Responsibilities	27

Computing Policies

Privacy	31
File Sharing & Copyright Violations	33
Printer Allocation	36
Emergency Coverage	37

What is this Guide for?

Welcome to the Technology Reference Guide, published by the Office for Information Technology (OIT). This handbook contains an overview of the computing services and resources available to the Williams community as well as a set of information guides on various computing topics. The goal of this publication is to provide an introduction to the information technology environment on the Williams campus. If you have any suggestions or comments about this publication or the oit web site, email oitweb-l@williams.edu. For online technical documentation, visit our wiki: <http://wiki.williams.edu/> and select the “Documentation” link from the list on the left.

The information in this handbook is current as of August, 2009. For the most up-to-date information, please visit the Williams OIT web site at <http://oit.williams.edu/>.



Faculty/Staff Support Desk: x4090

This Support Desk is the primary contact for faculty and staff technology questions. There are several people dedicated to answering the phones, but sometimes all lines are in use. If your call is not immediately answered, you may remain in a holding queue for the next available specialist, leave a voice-mail message, stop by the support desk at Jesup 210, or email Desktop Systems at desktop@williams.edu.

Academic hours: 8:00 am - 5:00 pm, Monday - Friday
Summer hours: 8:30 am - 5:00 pm, Monday - Friday

The help desk is closed but available to receive messages from 12:15 pm to 12:30 pm. For weekend and after-hours help, call the Student Support Desk (x3088), email stchelp@williams.edu, or email desktop@williams.edu. Although OIT can't guarantee a response off-hours, it's likely that an STC or Desktop Systems Specialist will read the email and offer help.

Student Support Desk: x3088

The Student Support Desk is the primary contact for student technology questions. It is staffed by Student Technology Consultants (STCs). Visit them on the first floor of Jesup, or email stchelp@williams.edu.

Academic Year Hours:

10 am - Midnight, Monday - Thursday
10 am - 8 pm, Friday
Noon - 6 pm, Saturday
Noon - Midnight, Sunday

Instructional Technology Liaisons

African-American Studies	Mika Hirai	x4328
Anthropology and Sociology	Sharron Macklin	x4318
Art / Art History / WCMA	Mika Hirai	x4328
Art History Graduate Program	Mika Hirai	x4328
Asian Studies - Chinese	Adam Wang	x4534
Asian Studies - Japanese	Mika Hirai	x4328
Astronomy	Trevor Murphy	x2231
Athletics / Dance	Jonathan Leamon	x4468
Biology	Trevor Murphy	x2231
Comparative Literature Program	Mika Hirai	x4328
Chemistry	Trevor Murphy	x2231
Classics	Chris Warren	x4323
Economics / CDE	Adam Wang	x4534
English	Mika Hirai	x4328
Environmental Studies	Sharron Macklin	x4318
Geosciences	Sharron Macklin	x4318
German-Russian	Mika Hirai	x4328
History	Sharron Macklin	x4318
History of Science	Trevor Murphy	x2231
Humanities	Jonathan Leamon	x4468
Latino/a Studies	Sharron Macklin	x4318
Leadership Studies	Sharron Macklin	x4318
Legal Studies	Sharron Macklin	x4318
Linguistics	Mika Hirai	x4328
Mathematics and Statistics	Adam Wang	x4534
Music	Trevor Murphy	x2231
Philosophy	Chris Warren	x4323
Physics	Trevor Murphy	x2231
Political Science	Sharron Macklin	x4318
Psychology	Adam Wang	x4534
Religion	Sharron Macklin	x4318
Romance Languages	Mika Hirai	x4328
Theatre	Jonathan Leamon	x4468
Williams-Mystic	Sharron Macklin	x4318
Williams-Oxford	Jonathan Leamon	x4468

Instructional Technology

Instructional Technology provides support for faculty interested in using technology in teaching and research. This includes:

- academic projects
- Williams Instructional Technology (WIT) summer intern program
- assistance with Blackboard (course management system)
- multimedia development and project assistance
- international television at **video.williams.edu**
- in-class workshops
- digital collections for teaching and research

If you have general questions about ITech services, please contact your department liaison (opposite), email **itech@williams.edu**, or call Jonathan Leamon at x4468.

Media Services: x2112

Facilities include:

- electronic classrooms
- major presentation venues (such as Chapin Hall or Brooks-Rogers)

Services include:

- training and consultation for using electronic classroom equipment
- support for lectures and presentations by faculty and guest speakers
- analog and digital video and audio format conversion and copying
- videotaping major college events for academic or college use

Media Services hours when classes are in session:

8 am - 9 pm, Monday - Thursday
8 am - 5 pm, Friday

Media Services is located in Jesup 317 and provides presentation facilities and related support for academic work and extra-curricular events.

Classrooms & Computer Labs

A current listing of our various facilities can be found at <http://oit.williams.edu/facilities/>. Classrooms and teaching labs can be reserved with the Registrar's Office through the drop/add period, and through the calendar office at <http://calendar.williams.edu/> for the remainder of the semester.

Electronic Classrooms

All registrar scheduled classrooms have a full set of presentation equipment, including a PC, a Mac, laptop connections, a CD/DVD/VHS player, audio system, and data projector. Some classrooms have slide projectors or document cameras, and most have transparency projectors. These rooms are scheduled by the Registrar's office.

Computer Classrooms, Open Labs, Specialty Labs

- Williams College has 7 computer classrooms. Four are PC labs: Bronfman 119, TPL 207, Schow 27 and Jesup 205; and two are Mac labs: Chemistry 216, and Jesup 207; plus a Mac/PC lab in the Center for Theatre and Dance.
- In addition, there are several open labs not scheduled as classrooms: Clark 201, Jesup 204, Kellogg Matt Cole library, and the Sawyer and Schow libraries.
- Specialty labs include a GIS lab (PC), a music composition lab (Mac), the language lab (Mac & PC), and a few other department-specific spaces.
- We also have a portable Mac lab which is a cart containing 21 Powerbook G4s. Contact Kate Fletcher at x2167 to schedule its use.

Collaboration Stations

Two Collaboration Stations are also available in the Science Center. One is located on the second floor bridge between the Thompson Chemistry Labs (TCL) and the Morley Science Labs (MSL), and the other is on the third floor of the Thompson Biology Labs (TBL).

These spaces provide:

- a large plasma screen with video inputs
- power outlets
- wired and wireless network connections

TeamSpot station

TeamSpot is a new technology that we're prototyping on campus this year that allows a group of users to work simultaneously and collaboratively on the same project. Bring your laptop to Jesup 204 and follow the directions to connect up to five users.

Media Studios

Williams has several facilities for multimedia development.

Jesup 101: staffed from 11am - 11pm seven days a week, by Student Media Consultants (SMC) trained in multimedia development.

Jesup 316: available from 8am - 5pm Monday through Friday and features a digital copy stand, media replication station and high-end printers for academic use.

Spencer 216: available 24x7 to students as well as faculty and staff that have card access to Spencer.

Technology Training

OIT Computing Workshops

Computing workshops are taught by OIT staff. Each workshop focuses on a given topic or application (Photoshop, HTML, etc). Classes are typically 90 minutes long, but shorter ones are also available. Introductory workshops assume no prior experience and cover everything you need to know to get started.

Our current workshop offerings can be found at <http://oit.williams.edu/workshops/>. Please sign up if you intend to come; workshops without a required minimum number of participants will be canceled.

In-Class Tutorials

Instructional Technology Specialists may be available for in-class workshops on these same topics.

Online Software Training: Element K

Williams College has a campus-wide license for Element K, a web-based software training service. You may take tutorials on any computer that has access to the Internet. The courses are available 24/7 and they can be

repeated or reviewed as often as you like. All you need is a compatible web browser. Information on how to sign up for Element K can also be found under the “Workshops & Training” menu item from the OIT home page.

Personal Blackboard Training

If you are a faculty member with questions about Blackboard features, or want a quick tutorial to get you started, contact your ITech liaison (see page 6) to schedule a one-on-one session.

Lynda.com

Lynda.com is another technology that OIT is experimenting with this year. It's an online service that helps users learn how to use various design programs like PhotoShop, Finalcut, Premiere, and InDesign with a focus on using these tools to create better finished products, be that images, videos, posters, web pages, etc. Lynda.com is available in Jesup 316.

Blackboard@Williams

Blackboard is a web-based course management system that is used for the majority of classes offered each semester at Williams. It provides easy-to-use templates and tools for faculty to put their course materials online. It also allows both synchronous and asynchronous online communication between faculty and students. Using Blackboard, Williams faculty can develop web-enhanced courses seamlessly and efficiently with no HTML knowledge.

Equipment Loan Center: x4091

Digital and analog equipment may be borrowed for academic or college use. Most equipment circulates for up to 3 days at a time. The Equipment Loan Center is located in Dodd Annex. We recommend making a reservation early, at least a few weeks in advance. The center can also be reached at eqloaning@williams.edu.

Academic hours: 9 am - Noon and 1 pm - 5 pm, Monday - Friday
Summer hours: 9 am - Noon, Monday - Friday

Equipment Inventory:

Digital Still Cameras	Data Projectors
Digital Video Cameras	MiniDisc Recorders
Tripods	Slide Projectors
Tape Recorder	Overhead Projectors
DVD/VCR Combo Units	PA Systems
Document Camera	Microphones
CD Component Players	Microphone Stands
Laptops (PC & Mac, Faculty only)	

Loaning Policy:

- Loaner equipment is for academic or college use by current Williams College faculty, staff, and students.
- The equipment must be returned before close of business on the appointed day (noon during the summer or 5 p.m. during the academic year).
- The person who checked out the equipment assumes financial responsibility for any damages or missing parts.
- The Equipment Loan Center does not offer blank media for any of the equipment.

Violations of the loaning policy could result in the loss of borrowing privileges. Persons who do not return equipment on time, three times, will have their borrowing privileges revoked until the beginning of the next academic year.

Williams Students Online: WSO

Williams Students Online (WSO) is an independent student organization at Williams College that creatively supports the computing needs of the College community. WSO Services include personal and student-organization web sites, listservs, interactive web tools, and computer instruction.

WSO holds weekly meetings. Newcomers are welcome; there's always room for more programmers, publicity folk, graphic designers, or people willing to learn.

You can access the WSO web site at <http://wso.williams.edu>. Suggestions and questions concerning WSO should go to wso@wso.williams.edu. More specific contact addresses include:

- listservers@wso.williams.edu - for questions about WSO listservs.
- [facebook@wso.williams.edu](https://www.facebook.com/wso.williams.edu) - for questions about the WSO facebook.

Purchasing a Computer

You can check the minimum specifications and the current recommended models at <http://oit.williams.edu/buycomputer/>. Computers that don't meet minimum specifications will still receive Help Desk support, but they invariably take longer to configure or repair and we cannot guarantee network connectivity. Questions regarding computer purchases can be sent to firstyear.techinfo@williams.edu.

Software

We strongly recommend that students purchase Microsoft Office (the Academic Standard version).

We are licensed to install Office (Word, Excel, Powerpoint, Outlook and Access) on home computers used for work by faculty and staff.

Anti-virus software is provided for all faculty, staff, and students. Keeping virus definition files up to date is required.

Other essential software may be downloaded from the Williams servers after connecting to the network. OIT provides a library of downloadable software available to current faculty, staff, and students for college related work (see page 25).



Passwords & Accounts

Changing Your Password

A single user name and password are used for most OIT services:

- email
- printing
- Blackboard
- the fileservers: Achilles, Hector, Helen, Athena, etc.
- web and FTP access to lanfiles.williams.edu
- access to the software application installers
- unix
- off-campus access of restricted services via the proxy server
- VPN

To change your password, select “My Account Settings” under the Help menu on the OIT home page. Note: this does not change your Meeting Maker, PeopleSoft, local windows account, or local OSX account passwords. OIT recommends that you use different passwords for these accounts.

Changing Your Local Account Password

Your computer has an account password as well that may be different than your Unix and Netware passwords. This password is used to access your local machine.

For XP:

From the START menu, select the control panel. Choose “user accounts.” Select your local account. Select “change my password.”

Note: If you change your Windows workstation password to your

Netware password, then it will login to the Windows account automatically after the Netware log in.

For OSX:

Under the Apple menu, select “system preferences” and choose “accounts.” Select the account and choose “edit.” Change the password.

Choosing a Password

It's important that no one knows or can guess your password. You might not have any important information that you need to protect, but if a hacker gets your password, s/he can initiate an attack on the Williams servers and network. Access to our servers is the first step in a hacker's ability to steal information and start a denial of service attack, which has occurred at Williams. Denial of service attacks can bring down our entire network. Remember: your password protects more than just your own data!

There are many available password-cracking programs. Words in the dictionary and/or standard combinations like “catdog” can be discovered in minutes. Also refrain from using your user name, family names, pet names, birthdates, etc. Do not use the same password for Williams accounts that you use at home or personal use. Passwords used for online registrations, purchases, downloads, etc. are too “public” to assume that they are secure for the Williams network. Mix in at least 1 number and 1 special character (;:!(@*][+=, etc). Example: “I cat=fur”. We require at least one numeral in the password.

Make sure whatever you choose can be easily remembered.

Email

Email Addresses

Email addresses are in the format: username@williams.edu and First.M.Last@williams.edu. All new user names are in the format initials + sequence number. For example, email sent to Ephraim.A.Williams@williams.edu and to eaw1@williams.edu go to the same account.

Selecting an Email Client

Every email client has a unique set of advantages and disadvantages. At OIT we are most familiar with Outlook, and OSX Mail, so we are able to support these clients easily.

Setting Up Your Client

Webmail (<http://webmail.williams.edu/>) requires no setup. Local email clients (Thunderbird, Outlook Express, etc) must be configured for your account and your mail server. The data you need is:

account:	your user name, e.g. jsmith or abc2
email address:	username@williams.edu
mail server:	facstaffmail.williams.edu or studentmail.williams.edu
SMTP server:	mail.williams.edu

Set both your incoming and outgoing mail servers to use a secure connection/communication of the SSL type.

Select IMAP

IMAP allows you to see the messages in your mailbox with the messages staying on the mail server until you delete them. When you check mail from more than one computer, you will see all of your messages.

IMAP folders live on the server, unlike local folders, which live on the local computer. To create a new IMAP folder, right click on the IMAP account (probably mail.williams.edu) and select New Folder. This folder is now visible to other computers you check your mail from. The habit of moving messages out of your inbox and into these IMAP folders will help you keep things organized.

Searching for Williams Email Addresses (LDAP)

New email clients use LDAP (Light Directory Access Protocol) to retrieve email addresses from a database. To add this service on a PC or Mac (Mac directions may deviate slightly), open Outlook Express even if you don't use it as your mail client. Once the configuration is done, you can look people up without using Outlook Express by going to Start:Search:For People.

1. Go to Tools:Accounts:Add button on right -> Directory Service.
2. Use server: ldap.williams.edu.
3. Do not check addresses using this service (all off-campus emails will fail).
4. Click Finish.
5. Select ldap.williams.edu on left, then Properties on the right.
6. Choose the Advanced tab.
7. In search base, put: ou= people, o=williams.

To look for an address, pull up Directory services from the Tools or Special menu.

Spam Filter

The Office for Information Technology has an Ironport server which checks our email for spam. There are several layers of protection available to you.

Our mail server checks incoming mail by identifying the server it is coming from. If the remote server is a known spammer then that connection is dropped immediately and the email is never delivered to your inbox. This method stops over 70% of the incoming spam.

The anti-spam software checks incoming mail for known subject lines or common spam types. When this spam is identified it places it in your quarantine file. You can access any email that has been quarantined by going to your account page at: <http://myspam.williams.edu>. The anti-spam software errs on the side of caution: the stated false positive rate is only 1 in 1,000,000, which is why some spam still gets through.

Some email clients, notably OSX Mail and Outlook 2003, have their own spam or junk mail filtering. Normally we recommend leaving this off, as the potential for false-positives outweighs the benefits of reducing your already minimized spam.

If you do receive an obvious email spam and there is an option to “click here to remove yourself from this list”, please do not do so. The link is most likely one that will only verify to the spammer that your email account is actively being read.

Speeding Up Email

Set your client to check for new email every 15 minutes. Setting it to 5 minutes or less will slow down the mail server for everyone, so please don't do that.

Keep your inbox small. The mail server must scan through the entire inbox every time you check for new email. Reduce your inbox by moving messages you want to save to other folders and delete and purge everything else.

The number of email messages you have is not the only issue. The number of attachments you received may be more of a burden. A simple email message that is text only would be only a few kilobytes in size. One email message with a Word document or a picture can be several megabytes in size.

Setting Up Automatic Email Replies (Absence Notices)

To activate absence mail:

1. Go to <http://webmail.williams.edu>.
2. Click on the “options” link in the upper right.
3. Select “Auto-reply” from the list on the left.
4. Select the “Yes” radio button, and enter your away message.
5. Click the “Apply” icon at the top left of the frame to activate.

Anyone who sends email to your account will receive back an email containing your automatic reply message. If you receive any listserv messages while auto-reply is activated, the entire listserv may get your away message. You may consider unsubscribing or suspending any listservs you are on.

To deactivate Absence Mail:

1. Go to <http://webmail.williams.edu>.
2. Click on the “options” link in the upper right.
3. Select “Auto-reply” from the list on the left.
4. Select the “No” radio button.
5. Click the “Apply” icon at the top left of the frame to save your changes.

Your recorded message will no longer be delivered.

Forwarding Email to Another Account

To activate email forwarding:

1. Go to <http://webmail.williams.edu>.
2. Click on the “options” link in the upper right.
3. Select “Forwarding” from the list on the left.
4. Select the “Yes” radio button, and enter the email address to which you would like to forward your messages.
5. Click the “Apply” icon at the top left of the frame to activate.

To deactivate email forwarding:

1. Go to <http://webmail.williams.edu>.
2. Click on the “options” link in the upper right.
3. Select “Forwarding” from the list on the left.
4. Select the “No” radio button.
5. Click the “Apply” icon at the top left of the frame to save your changes.

Viruses & Safe Computing

For general information about viruses and hoaxes, visit <http://www.vmyths.com/>.

Virus Scanners

We have a virus scanner that automatically checks the emails going through our system. Other email accounts (like Hotmail or Yahoo) which you can access while on our network are not being scanned by our server. This means that if you open an attachment from an alternate account your computer can become infected. Also bear in mind that anti-virus definitions always come out AFTER a virus is introduced to the Internet. There may be a one or two day delay between the propagation of the virus and our ability to detect it.

If a known virus is detected in your Williams email, the virus scanner will delete it, preventing infection.

Faculty and staff computers provided by OIT come with virus scanners installed. Students should install the anti-virus software provided to them by OIT.

A virus scanner is only as good as its definitions. Old virus definitions cannot adequately protect against the latest threats. Your virus scanner should automatically update when the computer is restarted. To update your Sophos Anti-Virus definitions manually, double-click the icon in the task bar that looks like a blue flower.

Safe Computing Practices

Following safe computing practices, along with an updated virus scanner, is your best defense:

- Maintain up to date antivirus software and software definitions.
- Scan all downloads and attachments for viruses before opening them.
- Do not open any attachments you weren't expecting to receive. If you don't want to delete it immediately, contact the sender to verify that the attachment is safe. Viruses "spoo" their return address. Even emails that appear to come from trusted colleagues and family members could contain viruses.
- Don't download software from the Internet and run it unless you trust the source.
- Beware of file sharing programs (Napster, BitTorrent, Gnutella, KaZaa, eMule, etc). The email virus scanner will not protect you from viruses obtained through those programs.

- Do no open email messages from "administrator" or "admin." All official messages from OIT will have the subject line "OIT Eph Notice mm/dd/yy."

Working From Off-Campus

From off-campus you can:

- Read and respond to your Williams email, as well as download, view and send attachments.
- Transfer files like Word and Excel documents from the Netware servers (your F: or G: drives for PCs, Hector and Helen for Macs) to your home computer or from home to college. You can also transfer files to and from the Unix servers.
- Access the restricted databases of the college libraries, like Lexis/Nexis, using the college proxy server. (Contact the library for more information.)
- View and modify your Meeting Maker calendar.
- Run Keyserved applications like Photoshop or Dreamweaver from a Williams owned laptop using VPN (Virtual Private Network).

You need to have:

- A computer (Mac or Windows) that is connected to the Internet.
- A modem for dialup (phone) access or an ethernet card for Time Warner cable or Verizon DSL.
- An ISP (Internet Service Provider) such as those listed below

The most common Williamstown ISPs are:

- Time Warner- a cable modem connection. Time Warner provides Internet access comparable to Williams' own high-speed connection, and costs about \$40/month.
- Verizon DSL- a DSL connection. It has similar speed and cost to Time Warner cable's service. It is not available everywhere, as the distance from a telephone junction is a limiting factor.

Checking Email

Webmail: From any web browser, such as Internet Explorer, connect to <http://webmail.williams.edu> and log in with your Unix user name and password.

Email clients. See the section on email for help on selecting and setting up an email client. When off-campus, you can choose to use your ISP's SMTP server (e.g. smtp.earthlink.net or you can use the Williams mail server (mail.williams.edu) using authentication.

Transferring Files (FTP)

Any FTP client can connect to **lanfiles.williams.edu** (which gets you to Hector or Helen). From there you can move files to and from your home computer. As with email, there are too many FTP clients to mention. On the Mac, Fetch is a common choice; on the PC, Core FTP is popular. Both Fetch and CoreFTP can be downloaded from <http://www.shareware.com/> or <http://www.download.com/>. We strongly recommend selecting the secure FTP or SFTP setting when using this type of software. It's required in order to access our wireless network.

Using Keyserved Applications

A Virtual Private Networking, (VPN) connection allows you to establish a Keyserver connection and run Williams licensed software from off-campus. The VPN connection is limited to faculty and staff. The software is also limited to Windows XP or Vista on the PC side and OSX on the Mac side.

The VPN connection requires Internet access to briefly connect to the keyserver. Time Warner cable or Verizon DSL is preferred, although a dial-up connection may end up working fine.

If your college provided laptop does not already have the VPN software you will need to download the Cisco Systems VPN Client from <http://oit.williams.edu/software/>.

Meeting Maker

For a home computer, we recommend using the web based client. Open your web browser and go to <http://mmserver.williams.edu/>. Follow the links to the Meeting Maker login. The browser may ask you to install a piece of java code from Meeting Maker; you should allow it to do so.

If you have a laptop that was set up by OIT with Meeting Maker, your client should work while off-campus.

Support

The OIT Help Desk is available to help with any of the functions described above. We are not able to diagnose problems due to ISPs or the hardware and software on a home computer. We would like to help, but the variations in home computers and ISP connections make diagnosis of these problems almost impossible over the phone.

There are highly qualified students available who can make house calls (for a consulting fee) and are capable of setting up the ISPs, email clients, FTP clients, and the proxy server.

Setting up Web Pages

Blackboard

There are many resources at OIT to help faculty place their course materials online. One of the most popular tools for this purpose is Blackboard, a web-based course management system that is typically used in more than half of the courses offered at Williams. It not only provides easy-to-use templates for faculty to put their course materials online easily but also provides tools that faculty can use to enhance their face-to-face classroom teaching and student-to-student interactions. These tools include class roster facebook, online discussion forum, course wiki and blog tool, electronic sign-up sheet, online assessment and gradebook. For more information, faculty should contact their department liaison (see page 6).

Department Web Sites

Academic and administrative department web sites are usually stored on the Unix server. You must obtain write-permission to the proper directory to add or update pages. Contact Heather Clemow of Public Affairs at x4065 for details. Note: there is separate space for files that need to be limited to on-campus access only.

Student Clubs and Group Web Sites

Student clubs and groups can obtain web space on **wso.williams.edu**. If your organization wants to have an account, one or more persons who currently have a personal WSO account should be designated as the official contact(s) with WSO. The contact persons are responsible for the content of the organization's pages.

To get a homepage for your organization, send e-mail to wso@wso.williams.edu and give the name of your organization and the names of everyone involved who needs access to edit the homepage. You will be assigned a subdirectory of the /home/www/orgs directory. The address of your organization page will be in the form <http://wso.williams.edu/orgs/orgname/>, such as <http://wso.williams.edu/orgs/wocl/>.

Personal Web Sites

Files that are in the public.www subdirectory in your directory (F: drive on the PC) on your Novell Netware server (Achilles, Helen, or Hector) are available to anyone who is using the Internet. You can also get to the same space by connecting to **lanfiles.williams.edu** with any FTP program. Your pages can be reached at <http://lanfiles.williams.edu/~yourUsername/>

yourFilename.fileExtension. If the entry page is named index.html, the address is simply <http://lanfiles.williams.edu/~yourUsername/>. Do what you wish with this space, so long as it conforms to the Computing Ethics & Responsibilities policy (see page 27).

OIT offers workshops and additional assistance to individuals who wish to learn how to create web pages (see page 9).

Listservs

List Administration

All current listservs use the web Listserv interface at <http://listserv.williams.edu/> to perform administrative functions. The listserv web site has complete manuals and documentation for subscribers and owners.

List Creation

Blackboard provides email lists for classes. Your instructional technology liaison (see page 6) can show you how. If you are a student looking to create a listserv for a student organization, contact WSO. You can request other types of lists by filling out the online request form on the ListServ guide available in the “FAQ” section of the OIT web site.

When you no longer need a list, please e-mail ListservAdmin@williams.edu to request its removal. In the message please provide your name, phone number, or other means of contact in case we have any questions or problems.

Wireless

The Office for Information Technology is pleased to provide a wireless network connection to registered users of the Williams Network. Wireless is available in all campus buildings. It is available outdoors where you are close enough to a building to connect. Please report any in-building locations where you can't connect so that we can fix them.

Connecting to the Wireless Network

You will need to log in to the wireless network in order to connect. The method for doing that is changing and the procedure is not defined as of the printing date of this guide. Please check the OIT web site at <http://oit.williams.edu/wireless/> for instructions.

Using the Wireless Network

Wireless connections are inherently insecure, so we will require the use of secure applications when connecting to Williams servers. For example, you will need to use:

- Secure Shell (SSH) instead of Telnet, use Putty on the PC and SSH on the Mac.
- Secure FTP (SFTP) instead of FTP, use Core FTP on the PC and Fetch on the Mac.
- Secure POP email (S-POP) instead of regular POP3 email.
- Secure IMAP email (S-IMAP) instead of regular IMAP email.
- Set your incoming and outgoing mail servers to use SSL.

You would be wise to use these secure connections even when not absolutely needed.

More information is available at <http://oit.williams.edu/wireless/>.

Data Storage on File Servers

Personal File Server Space

All Williams users have their own personal file and web space on one of the Novell Netware servers: Achilles for students; Helen or Hector for Faculty and Staff; Jasper for OIT staff. New accounts are created with 150 MB of space. On Dell computers configured by OIT, this space is configured as the F: drive. The space is also accessible by FTP at lanfiles.williams.edu.

Department File Server Space

Departments may share files using space on one of the Novell Netware servers. On PCs, this is the G: drive. The space is configured so everyone can share some files, and other files can be limited to individuals or groups. Contact the Faculty/Staff Support Desk at x4090 for more information.

Academic Project Storage Space

The “Projects” server can be used for short or long-term storage of large files to be used in classes or research. Faculty should contact their instructional technology liaison (see page 6) for more information.

You can also get personal and departmental shared space on the web. Go to <http://netstorage.williams.edu/> and log in using your user name and password. You will be able to see your personal and shared space, and upload and download files. You will NOT be able to get to the “Projects” server.

Backing up Data

There are two types of files:

- Data files that you create (Word documents, Excel spreadsheets, pictures, etc.)
- Programs that you use to create your work (Word, Excel, Photoshop, etc.)

There is no need to backup the program files; they can be reinstalled. The important data is in the files that you worked hard to create. You should keep multiple copies of your files in different physical locations.

Organize your data so the backup procedure is quick and efficient:

- Keep all your data together: move all the files and folders/ directories you want to backup into My Documents (or a similar folder) on your hard drive.
- Make sure any new files you create are saved in there as well.

You can store your backup data on personal media or the Williams Netware servers such as Helen, Hector, or Achilles (represented by drive letter F: on a PC). Examples of personal media:

- recordable CDs & DVDs (CD-RW or CD-R)
- external (USB 2 or Firewire) hard drives
- zip disks (not recommended)
- floppy disks (not recommended)

NetWare servers provide additional protection, because servers are backed up nightly. However, keep in mind that daily server backups are retained for one month. It would be impossible to retrieve a file from our server backup that you deleted two months ago.

Green Computing

Green (i.e. sustainable) computing is about finding a balance between what we need to do and the impact that has on the environment. There are three main considerations in green computing: the energy the computer system uses; the resources used indirectly when working on the computer (ranging from paper for printing to the air conditioning that keeps the machines from over-heating); and what happens to old equipment when it's replaced or no longer needed.

OIT manages the institutional systems and supports programs with this

in mind, but there are steps individual users can take as well. The three quickest and easiest things you can do are:

- Turn off (or hibernate / deep sleep) your computer. Whether you're away from your room for the day, or out of your office for the night, shut down your machine before you leave (or set it to shut down automatically). You will not hurt your computer by turning it off and on each day.
- Don't use a screen saver. For many people the screen saver is the most energy consuming application they run. Instead, have your screen go blank, or better yet actually go to sleep (set via the power management system for your computer) - it uses less energy and it's better for the screen.
- Don't print what you don't need. Williams goes through incredible amounts of paper, and much of it is never even picked up from the printer. Print double sided if your situation allows, print only the necessary pages, and pick up and use what you do print.

More information about Green Computing at Williams is available in the college wiki: <http://wiki.williams.edu/display/docs/Green+Computing>

Downloading Software

OIT provides a library of downloadable software available to current faculty, staff, and students for college related work. Most of the applications are controlled by a license manager called KeyServer. Therefore, your computer must be connected to the Williams network and have the KeyServer client installed for the application to run.

Installing Software

1. Visit <http://oit.williams.edu/software/> to see the list of available software.
2. Make sure you have the KeyServer client installed.
 - If your computer was set up by OIT, you already have it.
 - If you do not have it installed, download "KeyServer client"
3. Find the software you want to download, and click on the appropriate icon (Windows or Mac) to download it.
4. An installer will appear on your desktop. Run the installer. You may need to restart your computer before the application is available.

Printing to a Network Printer

Williams uses a print server so you can print to networked printers all over campus. The print server also helps us monitor the environmental impact of campus printing. You will need to install a client on your computer to access public campus printers. Instructions on how to set up campus printing can be found at <http://print.williams.edu/>.

Duplex Printing

Many printers on campus support duplex printing (printing on both sides of a sheet of paper). Please use this option unless you really need single sided printing. Duplex is the default on public lab printers that support it.



In order to use the Williams network and computer systems, you must agree to these.

Computing Ethics & Responsibilities

Williams College provides computing and networking resources to students, faculty, and staff for a wide variety of purposes. These resources, networked for the general benefit of the community, are continually updated and maintained to provide an academic environment that is consistent with the educational goals of the College. These resources are limited, and how each individual uses them may affect the work of other members of the community and beyond, as our campus network is connected (through the Internet) to other networks worldwide. It is important that everyone be aware of his or her individual obligations and what constitutes proper use and behavior.

Williams College Computing Ethics and Responsibilities are available in the Student Handbook, the Administrative Handbook, and other publications of the College, as well as the Williams web site. Because of the rapid evolution of computing and information networks, the College reserves the right to modify these policies, with approval of the campus-wide Information Technology Committee, and publish the latest version on the OIT web pages. While users will be kept apprised of any changes, it is the user's responsibility to remain aware of current policies.

Common sense is a good guide to what constitutes appropriate behavior and use of computers and networks. You should respect the privacy of others and use computing resources in a manner that is consistent with the educational objectives of the College.

Behaviors that can create problems in a networked computing environment fall into the categories below. This list of responsibilities,

while not exhaustive, should provide users with a good idea of what constitutes illegal or unethical on-line behavior. Users should note that computer users are governed by federal and state laws, including copyright laws, and College policies and standards of conduct.

Violations of these rules or, indeed, any disruptive situation in which a person's behavior or behavior generated on machines, accounts, or file space under that individual's control, creates a disruption of service to our clients, may be met by suspending access and services to the responsible parties. Access and services may only be restored following a discussion with the Office for Information Technology (OIT) and, if appropriate, other officers of the College.

When there is reason to believe that illegal activities or significant infractions of our rules have occurred or are continuing, with the permission of the appropriate senior officer of the College, OIT staff may monitor a suspected individual's computer files and activities. When necessary, the College may invoke the assistance of a law enforcement agency. The Office for Information Technology will not judge whether any request from a law enforcement agency to investigate suspected illegal activities affords due process and is of appropriate jurisdiction; OIT defers such requests to the appropriate officers of the College, and provides information required by subpoenas from courts with proper jurisdiction.

Break-ins

You may not attempt to gain access to computer systems (on or off campus) for which you have not been explicitly granted access.

Tampering

You may not deliberately attempt to disrupt the performance of a computer system or a network, on or off campus. You may not attempt to 'break' system security. You may not reconfigure computer systems to make them unusable for others. You may not attempt to destroy or alter data or programs belonging to other users. You may not modify residential computing network services or wiring or extend those beyond the area of their intended use. This applies to all network wiring, hardware, and cluster and in-room jacks. Gateways and firewalls designed for home use, such as Cable/DSL routers and Wireless Access Points, can disrupt the normal operation of the Williams network and are not allowed. You are responsible for protecting your computer and not allowing others to use your computer to attack others on the network. Specifically this means that you are required to be running a supported, up-to-date, anti-virus package and to ensure that your computer has had all applicable security patches installed.

Theft

By the copyright laws of the United States and most other nations, virtually all information in computer files is copyrighted.

If you have not been given direct permission to copy a file, you are not permitted to do so. You may not copy or redistribute software or other information that is copyrighted. By US law, software piracy is a felony. You may not attempt to override copy protection on commercial software. The ability to find and read information on computer systems does not mean that the information is in the public domain. Having the ability to read does not necessarily grant the right to copy or redistribute. Nor, even, in the case of certain information on the Internet, does ability to read mean that permission to read has been lawfully granted. Certain information is licensed to be read by the Williams community, though this does not grant the right to redistribute this information. See remarks under Eavesdropping and Violations of Privacy, below.

Eavesdropping and Violations of Privacy

All information on a computer system belongs to someone; some of it may be private or personal information; some may consist of confidential information, trade secrets, or classified material. If you have not been given direct permission to read or access another person's file, you may not try to do so. The Williams network is a computing system covered by this policy. The operation of packet capture or port scanning software, or other means of snooping on other's network activity, is strictly forbidden. Williams-specific or commercially obtained network resources may not be retransmitted outside of the College community. Examples include copyrighted course materials, electronic journals, other commercial information services from the Williams College Library, and private student and/or employee-related information such as home phone numbers, addresses, and photographs of students.

Forging, Password Sharing, Password Stealing

You may not attempt to impersonate another individual by sending forged information such as e-mail. Never give your password to anyone or use another's password. You may not seek to determine another person's password, through cracking, decryption, interception or other means.

Annoyance and Harassment

Williams College has written standards of conduct that seek to prohibit annoyance and harassment by any members of the Williams College community.

You may not use computing resources to violate the College's standards of conduct. You may not distribute electronic chain letters or spam.

These are not only annoying, but can also severely disrupt computing and network performance.

Negligence and Misuse (including private business)

Having access to computing privileges (e-mail account, Williams network connection, login, or shared file space owned by you), means that you have general responsibility for all computing activity which takes place from those accounts, connections, or file spaces. The College's connection to the Internet, for example, does not allow you to abuse that connection.

Access to the Williams College computing network and the Internet is limited to members of the Williams College community. Individuals within the Williams community are not permitted to provide access to the campus network to those outside this community. This restriction includes the operation of server software to provide any service that is accessible by those outside the Williams network without permission from OIT. Use of Williams Computing facilities is intended to be consistent with the educational mission of the College; this does not preclude personal uses. However, we note that the College has:

- for students: "Regulations covering student businesses" in the Student Handbook
- for faculty: "Other employment during the academic year" in the Faculty Handbook
- for administrative staff: "Employment outside Williams or beyond full-time with the College" in the Administrative Staff handbook

All place some limitations on the community's use of computing facilities for commercial purposes.

You should report any suspected illegal or unethical activity to the Office for Information Technology or the Dean's Office.

Copyright and Attribution Reminders

Receiving, possessing, or distributing copyrighted material without the permission of the copyright holder is prohibited. Such acts are also a violation of the laws of the United States. Violators of copyright law could be subject to felony charges in state or federal court, and may also be sued by the copyright holder in civil court. To learn more about copyright, visit the Library's web page about copyright:

<http://library.williams.edu/copyright.php>

Illegal file-sharing using peer-2-peer file sharing programs is strictly prohibited both by College policy and under the Digital Millennium Copyright Act of 1998 ("DMCA"). The DMCA limits the liability of internet service and network providers (ISPs), including the College in its role as an ISP, in disputes between copyright holders and users of those services. The DMCA also establishes procedures through which copyright

holders can obtain information from internet service and network providers about alleged infringing use of those services. These procedures make individual students, faculty and staff responsible for their illegal file sharing, and they must assume all resulting liabilities as individuals without support from the College. To learn more about how the College handles DMCA notices from the entertainment, music and other copyright holders, read our policy about File Sharing and Copyright Violations.

Privacy

Technology users at Williams College have a right to privacy. OIT respects and protects your privacy, but may be required to release information if we receive a legal subpoena or we are contacted by Senior Staff that you have violated College policy. In order to help ensure privacy for all users, the Office for Information Technology (OIT) employs passwords associated with user accounts. As users of technology at Williams, you also have a responsibility to guard your account and keep your password to yourself.

The secrecy of your password is critical to the integrity of the campus computing environment. If an intruder is able to gain access to one account on a system because that account's password was simple to guess, the intruder can then often determine other users' passwords. For this reason you must keep your password secure.

No computer system can protect you if you do not conceal your password. Leaving a terminal without logging off is like leaving the door of your home unlocked and open. Using an obvious password, such as your first name or a nickname, is like hiding your door key under the doormat. Use a combination of eight or more letters and numbers to confound anyone seeking access to your data. And change your password often. At the very least the systems will require you to change your password every six months. If you are unsure about how to change your password, please contact the Jesup help desks (x4090 for faculty/staff, X3088 for students) for assistance.

Systems Administrators

Activity logs are maintained on all systems managed by OIT. Information that is logged includes at minimum the login and logout time of every user. Additional information may be logged on specific systems. For example web-server logs record what pages are visited and the referring link. (This is not special to Williams's web-servers; all web-servers on the Internet log this information). Email logs record the fact that a message was sent, the submission time and the delivery time, and the addresses of sender

and recipient. Content of email is NOT logged.

System logs are not routinely monitored, but are used for troubleshooting purposes when a problem has occurred. Reports may be generated of aggregated information without reference to specific users.

System level privileges are granted to OIT staff who need them to perform their jobs. These staff are responsible for safeguarding the system and the information within it. They respect the privacy of personal files and mail within the system. The Office for Information Technology makes a concerted effort to protect user privacy and to prevent unauthorized use of the Williams system.

Systems may be monitored if there are suspected abuses or violations of college policy and individuals may be identified. When there is reason to believe that illegal activities or significant infractions of college rules have occurred or are continuing, OIT may monitor a suspected individual's computer files and activities. Such action may be taken at the request of Security or Human Resources, but must in all cases have the consent of a member of the college's Senior Staff.

If OIT staff receive a subpoena or are contacted about violations of the PATRIOT Act, the Chief Technology Officer will contact the appropriate Senior Staff member and seek legal confirmation that the requests are valid. Although ordinarily Williams does not track Internet use, users should be aware that activity on the Internet can be tracked at other Internet locations through IP addresses and traced back to their machines.

Any attempt to interfere with or to alter the integrity of any computer system is unacceptable. Such actions include, but are not limited to:

- unauthorized use of accounts
- impersonation of other individuals in communications
- attempts to capture or crack passwords
- attempts to break encryption protocols
- causing unreasonable network bandwidth congestion
- compromising privacy
- destruction or alteration of data or programs belonging to other users

Members of the Williams community should respect the security and access policies of other systems as well as the desire of other institutions to safeguard themselves against intrusions.

Violation of Computing at Williams policies or procedures may result in the revocation of your computing privileges and/or other disciplinary action.

Public Computer Monitoring

Public kiosk, lectern, lab, and classroom computers have monitoring software running on them. This software records who logs in where, for how long, and what applications are used, but not what is done with those applications. E.g. the system records would show that the Firefox web browser was in use for 35 minutes, but NOT what sites were visited during that time.

The data collected is primarily used in an anonymous fashion for support purposes (e.g. what applications are most commonly used, which labs receive the most use and therefore might need more computers, etc.), but in the event of a subpoena, security breach, hacking from one of our computers, or other such special circumstance individual sessions may be examined in detail.

File Sharing & Copyright Violations

Your computer may be uploading music without your knowing it.

Current technology easily allows your personal computer to duplicate and distribute copyrighted video images, audio recordings and other digital materials. Unfortunately this makes it is easy for you to violate College policy and US copyright law. For this reason you should know the use of popular and freely distributed file sharing programs to download copyrighted music and video material, in almost every case, places you in violation of College policy and U.S. law.

Most of these programs by default allow Internet users to copy files from your computer. Most programs don't alert you in advance or even ask your permission before turning your computer into an Internet file server. Some of these programs also install hidden components that allow file sharing to run in the background on your computer. As a result, whenever your computer is turned on, the file sharing application is also enabled, even if you don't open the application or actively use the program. They also open up a back door to your computer for viruses and worms. This places you at great risk of violating college policy and copyright law by becoming an unlawful distributor of copyrighted material. For example, what you may believe to be a single one-time policy violation consisting of downloading a single track of music from a popular CD is actually an around-the-clock violation of College policy and copyright law because any time your computer is turned on it is publicly announcing to the Internet (perhaps unknowingly to you) that the single music track you previously downloaded is now available on your computer for distribution via the Williams College network. Because the College has a reliable and

large capacity connection to the Internet and because these file sharing programs favor computers connected to fast reliable networks, thousands of other Internet users flock to your computer to download your file. You can learn more about how to protect yourself from uploading files inadvertently at http://www.musicunited.org/5_takeoff.html.

OIT does not monitor normal computer use

OIT staff do not monitor computer use on the College network to look for copyright violations, but in the process of investigating network congestion or troubleshooting technical problems, they may become aware of policy violations. In such cases the OIT staff member will report these violations to the Chief Technology Officer who will consult with the Associate Dean of the College, the Director of Human Resources or the Dean of the Faculty.

The entertainment industry is aggressively seeking out copyright law violators

You also need to be acutely aware that law enforcement agencies, the Recording Industry Association of America (RIAA), and other copyright holders of digital media such as HBO, Universal Studios, the Business Software Alliance, and the Entertainment Software Association actively monitor the Internet for users who are distributing copyrighted material. The recording, film and software industries have recently become very aggressive in their active pursuit of copyright infringement. They have spent millions of dollars, and they have hired hi-tech firms to develop and maintain software that is able to search the Internet and identify unauthorized distribution of their protected titles. This active monitoring is specifically designed to search for distribution of materials using the most commonly used software packages.

How Williams College handles Digital Millennium Copyright Act (DMCA) notices or early settlement letters

In the 2006-2007 academic year, Williams received almost 100 formal complaints from legal authorities representing copyright holders stating that computers on the College network were involved in the unlawful distribution of copyrighted materials. Each case was easily traced back to a computer connected to the campus network, running one of the common file sharing programs. Many of the cases involved unsophisticated and first-time use of these programs. It is clearly not safe to assume that even the most casual copyright policy violation will go undetected.

When a copyright holder or their agent contacts Williams about an occurrence of copyright violation with a standard DMCA notice, the school is required to take action. If you are suspected of infringement, the College's DMCA agent, the Chief Technology Officer, will confront you about the matter with an email notice. If you believe you are not

responsible for the offending computer, you should notify the Chief Technology Officer immediately. If you are a student, all computers and other devices registered in your name will be removed from the Williams College network automatically for a period of one week once the Chief Technology Officer sends you the notice (or starting the next business day if the notice is sent on a weekend or holiday). You must respond to the Chief Technology Officer promptly that you have blocked access to the offending files or your computers and other devices will remain off the Williams College network indefinitely until she hears from you. If you are a faculty or staff member, the Chief Technology Officer will not immediately remove your computer from the network, but will notify the Dean of the Faculty (for faculty) or your supervisor and department head (for staff). But you must also respond promptly to the Chief Technology Officer that you have blocked access to the offending files or your computer will be removed from the Williams College network until she hears from you.

If you receive a notice and do not block access to the file(s), you have the right to petition the College to restore the computer to the network (for students, after the one-week College penalty), which it would do, while you pursued the matter legally with the alleged copyright holder or its designated agent.

If you block access to the file and notify the Chief Technology Officer, you do not need to respond to the agency sending the notice. Correspondence to this point is between the College and the agency, which does not have your identity. We will identify you to them only if they issue us a legal subpoena.

In March 2007 the RIAA began pursuing students more aggressively by sending out early settlement letters. A letter explaining this development was sent to all students in April 2007 by the Chief Technology Officer and the Associate Dean of the College. A similar letter was sent to faculty and staff. The DMCA notices we received in the past required you to remove or block access to the file. The new early settlement letters ask that you preserve but disable the software and the files. The College will not help or advise you in this process so, if you receive such a letter, you might wish to contact an attorney for assistance about how to respond.

In October 2007 the Chief Technology Officer, the Associate Dean of the College, the Dean of the Faculty and the Director of Human Resources sent second letters to returning students, faculty and staff. The letters updated the community on settlement letters and a subpoena received by the College. A similar letter had been sent to first-years in August before they arrived on campus urging them to delete their file sharing (P2P) programs before they came to campus.

Everyone must abide by copyright restrictions and the College's

acceptable use policies as stated in our Computing Ethics and Responsibilities. By installing and running these common file sharing applications you put yourself at great risk, and unless you are technically sure your use of such programs is not a violation of College policy or the law, we strongly encourage you to avoid their use.

Please keep in mind that you are responsible for all uses of your computer, and that network use by a computer can be traced to its registered owner.

Printer Allocation

OIT will provide networked, postscript-capable, laser printers for workgroups. Printers will be located such that there is a workgroup printer convenient to all college employees who make use of printing. In the case of departmental chairs, department administrative assistants, and senior staff, personal laser printers will be provided.

If a faculty member or department has an unusual computing need that would require an exception to the procedures listed above (i.e. a dye sublimation printer for high-quality color images), OIT management will call a working group to evaluate the situation and make a recommendation. If possible these occurrences should be used to add to this guidelines document.

If a faculty member or department wishes to purchase a local printer for an individual not provided with one under our guidelines, OIT will recommend a printer that we can support but will not provide funds. If a printer not on our list of supported printers is purchased, it will be understood that support by OIT for problems encountered will be quite limited.

If a faculty member or department decides to install a non-approved printer with their own funds, such a printer can be attached to the network as a local workgroup solution but will not be configured with server-based queues, either Novell or Unix. Additionally, drivers for such a printer will not be installed and maintained in a central location on the college's fileservers.

A departmentally purchased printer will be supported by OIT only on a casual basis. In other words, OIT staff will not be expected to be expert in the operation of such a printer and any support provided will take a lower priority status than other support calls. Within those parameters, we will do our best to help out.

All queue based networked printers will be named in a way that identifies

the type of printer and its location. The names will be of the form:

Type-building-roomnumber (-numericidentifier if necessary)

For example: lw-jesup-205 would represent a Postscript printer in Jesup room 205.

OIT encourages departmentally and personally purchased printers placed on the network to be named in conformance with our naming standards. Failure to do so will hamper our ability to provide what support we can to such printers.

The list of approved, supported, printers will be reviewed periodically by an OIT working group. At any time, new printers could be evaluated and beta-tested for possible inclusion on the approved list. At review time, older printers could be retired from the list and newly tested printers considered for inclusion. The testing process would consist of at least:

- Testing on the network by Jesup staff at OIT.
- Beta-testing in a heavy-use workgroup environment by an appropriate department for at least one semester.

Emergency Coverage

When the college is officially closed for non-essential personnel or when offices are closed but classes are in session, OIT will make every attempt to provide the following coverage:

Staff on-site:

- Two people from Networks and Systems
- One person from Desktop Systems
- One person from Instructional Technology

Staff reachable by phone/pager and who will have remote access:

- All Networks and Systems staff
- Representatives from Administrative Information Systems
- Representatives from Desktop Systems
- Representatives from Instructional Technology

When the college is closed for inclement weather and hazardous driving, the on-site representative from each group will preferably live within walking distance or minimal driving distance. Each semester, the specific individuals will be identified and the plan will be reviewed with them.

When offices are closed and classes are not in session, no OIT staff will be required on-site. Normal weekend and evening coverage using phone/pagers and remote access will be in effect.

oit contacts

Fac/Staff Support	x4090
Student Support	x3088
Media Services	x2112
Equipment Loan Center	x4091

Web site <http://oit.williams.edu/>

ACADEMIC YEAR HOURS

	Mon-Thu	Fri	Sat	Sun
Fac/Staff Support	8am-5pm	8am-5pm	Closed	Closed
Student Support	10am-12am	10am-8pm	12pm-6pm	12pm-12am
Media Services	8am-9pm	8am-4:30pm	Closed	Closed
Equip. Loan Center	9am-5pm	9am-5pm	Closed	Closed
Jesup101	11am-11pm	11am-11pm	11am-11pm	11am-11pm

The Technology Reference Guide is published by the Office for Information Technology. This handbook is a document for the private use of the Williams community. Copyright by Williams College, all rights reserved.