Information Technology Handbook 2008-2009

Department of Information Technology
Web: www.smcvt.edu/itweb
Email: ithelp@smcvt.edu
Helpdesk: 802-654-2020

Welcome

to

Information Technology @ SMC

The Department of Information Technology (IT) is committed to creating a robust technology environment for the students, faculty, and staff of Saint Michael's College. We support the mission and goals of the college with tools and services for our campus constituents: a reliable, secure, and fast campus network; support for the appropriate integration of technology into teaching and research; and the technology support for operations of the College. The IT portfolio includes administrative and academic software applications; network, cable television and telecommunication services; helpdesk; Web support; and media resources. Working closely with faculty, staff and students, IT functions as an advocate for the intelligent and effective use of technology on campus. The department has a strong commitment to quality service, continuous improvement and innovation. Please feel free to contact us to talk about Information Technology and the services we offer.

The campus network, Mikenet, provides connectivity to network resources, including full Internet access, electronic mail and network printing. All labs, classrooms, offices, and residential areas are fully wired and have access to the campus computer network (Mikenet), telephone services and cable services. Telephone service in classroom areas is limited to support phones in electronic classrooms.

- **Enterprise Application Support.** *This group supports the institutional applications, including the Library cataloging system, security and administrative applications. Headed by Erin Slattery.*
- **Instructional Technology Services**. *ITS provides services designed to help faculty enhance their teaching and learning with technology, and includes media services, academic web development, classroom technology support, instructional support, support for specialized labs and technology training on both an individual and small group basis. Headed by Susan Breeyear.*
- **Networking Services.** *This service area provides management and support of the College network servers, services and infrastructure. Headed by Rick Murphy.*
- **Telecommunications.** *This service area supports the telephone, voicemail, cable TV and satellite services on campus. Headed by Andy Day.*
- **User Services**. *This service area combines the services of the Helpdesk, technology procurement and IT communications. This group is responsible for desktop and user support for the campus community. Headed by Joann Trottier.*

What's New!

- ***Helpdesk phone system:*** To better serve you, we've implemented an IPT phone system at the Helpdesk. Some key enhancements include:
  - Your call is automatically routed to the most skilled technician available.
  - When you leave a voice message, an IT work order will be automatically created for you and you'll receive an email confirmation with the work order number.
  - When you call the Helpdesk, you'll be alerted when there is a service interruption or an emergency closing and you can listen to our IT Status Line for additional information.

- ***NEW Vendor! Saint Michael's College Student Laptop Program***
  - In partnership with CampusHP, Saint Michael's College has implemented this special program for students that includes full business-class hardware and software support at very reasonable academic discount pricing. CampusHP Student Care software support and Accidental Damage Protection are included with the HP laptops purchased through this program for four full years. You'll find details about the program on the web at www.campushp.com/smcvt .
  - **On-Site Support:** A CampusHP technician will have an office at the Helpdesk and will provide on-site support for laptops purchased through the CampusHP program as well as hardware warranty service for HP, Lenovo, MPC/Gateway and Apple computers. CampusHP provides malware support as part of the Student Care support package included in the Student Laptop Program; for other computers, CampusHP will provide this service for a fee.

- ***Expanded wireless:*** In addition to the Library, Jeanmarie Hall, Cheray Science and Alliot, wireless has been expanded to the following areas:
  - Saint Edmund's Hall classrooms
  - Hoehl Welcome Center
  - Sutton Fire House
  - Tarrent Hall of Fame Room and the Field House

- ***New computers in labs and classrooms:*** New HP workstation computers have been placed in the multimedia labs in Jeanmarie and Bergeron. New HP desktop computers are in all of the classrooms and public labs.

- ***New computer labs and network printers in the residence halls:*** In addition to new computers in the Linnehan, Purtill and Hamel residence halls, new computer labs and network printers have been placed in Alumni, Ryan, Lyon, Joyce, Founders, Canterbury, Pontigny and Cashman.

Office Hours and Locations

The Department of Information Technology offices are located in three areas on campus: the second floor of Saint Edmund's Hall, and the second and third floor of Jeanmarie Hall. Staff offices, the Helpdesk, the Language Learning Resource Center, and Media Services are located in these areas.

- ***IT Offices,*** Jeanmarie 278, x2604
  Monday-Friday, 8:00AM-5:00PM

- ***Helpdesk,*** Saint Edmund's 221C, x2020
  Monday-Thursday, 7:30AM - 7:30PM
  Fridays, 7:30AM - 3:30PM
  Summer and holiday hours: Monday-Friday 7:30AM-4:30PM

  The Helpdesk is located in Saint Edmund's Hall, Room 221C. The Helpdesk provides phone, walk-in and email support for students, faculty and staff. On campus, dial ext. 2020 to reach the Helpdesk; from off campus, dial 802-654-2020. Inquiries may also be directed via email to ithelp@smcvt.edu. ***Ask IT!***

- ***LLRC (Language Learning Resource Center)***, Saint Edmund's 215, x2381
  Monday-Thursday, 8:00 AM – 8:00 PM
  Friday, 8:00 AM – 5:00 PM (see website for schedule changes)
  Summer and holiday hours: 8:00 AM – 5:00 PM

  The LLRC provides technological support for students learning a second or foreign language. A combination of wired and wireless laptop computers, flexible seating, media equipment, and dedicated staff provide a state-of-the-art environment for classroom instruction, individual study or collaborative work. The LLRC offers specialized language software, a lending library of ESL and modern language materials, and a collection of foreign and domestic DVD's chosen for their language-learning qualities. Online audio files for student use are also provided through the LLRC.

- ***Media Services,*** Jeanmarie 387, x1919
  Monday-Friday, 7:30 AM – 5:00 PM, weekend hours as needed

  Media Services provides media equipment consultation and support to the campus in general, and to the classrooms in particular. A variety of multimedia resources are available for setup in non-tech classrooms and for campus presentations. Arrangements for equipment setup in classrooms may be made by dialing x1919 (654-1919 off-campus); non-academic setups should be arranged through the Special Events office, x2615 (654-2615 off-campus).

Information Technology Staff Listing

	Ext.	Location
Chief Information Officer (William Anderson)	2252	SE 221B
Director of Information Technology (Billie Miles)	2930	JE 274
Administrative Assistant (Bernie Ravenelle)	2604	JE 278
Enterprise Applications		
Assistant Director: Enterprise Applications (Erin Slattery)	2226	JE 268
Applications Development Specialist (Peter Cross)	2691	JE 262
Middleware Developer (John Connors)	2225	JE 266
Instructional Technology Services		
Assistant Director: Instructional Technology (Sue Breeyear)	2821	SE 219B
Instructional Technologist/Manager LLRC (Kelley Taplin)	2878	SE 213
Instructional Technologist (Cynthia Kelley)	2756	JE 260
Senior Media Specialist (Richard Leggett)	1919	JE 387
Senior Instructional Support Specialist (James Millard)	2983	JE 286B
Networking Services		
Senior Network Administrator (Joe Pawlaczyk)	2229	JE266
Assistant Director: Networking (Richard Murphy)	2233	JE 272
Systems and Network Specialist (James Peterson)	2433	SE 221D
Telecommunications Services		
Telecommunications Specialist (Andrew Day)	2552	JE 270
Telecommunications Specialist (Patricia White)	2729	JE264
User Services		
Associate Director: User Services (Joann Trottier)	2515	SE 221A
Senior User Services Specialist (Andrew Churchill)	2418	SE 221I
Desktop Services Specialist (Shawn Umansky)	2763	SE 221G
Helpdesk Services Manager (Erik Lightbody)	2020	SE 221C

Knightvision, Mikenet, or eCollege?
Demystifying technology accounts at SMC

Whether you're a new student, faculty, or staff member at Saint Michaels, your technology accounts will be important to you. This document is an attempt to explain how to acquire accounts, access them, and get help when you need it.

Mikenet
Mikenet is the Saint Michaels College campus network. Mikenet resources include email, webmail, personal and/or academic website space, a network share for storing files, use of campus computers, access to library resources, networked printing on campus, and access to wireless computing.

Access
All new undergraduate students, and most new faculty and salaried staff members, will automatically receive a Mikenet account when they arrive. Graduate students, hourly staff members, and adjunct faculty may need to request a Mikenet account through the IT Helpdesk (x2020) or by filling out the request form found on the web. Before requesting a Mikenet account, employees should make sure all their paperwork for employment has been filled out, signed, and returned to the Human Resources office. A Mikenet account is a prerequisite for most other types of accounts on campus.

Getting Help
For help with Mikenet accounts, contact the IT Helpdesk at x2020, or send an email message to ithelp@smcvt.edu. Make sure you include your return phone number in the email request.

eCollege
eCollege is the official course management system at Saint Michaels, currently used by about 60% of its faculty. Faculty members post assignments, resources, announcements, current grades, and other information for their students about each of their courses on eCollege. Students can post papers, participate in discussion groups, and share web resources, among other things.

Access
eCollege student accounts are automatically generated when a student signs up for an eCollege-designated course. Usernames and passwords are unique. Students who add eCollege courses after the beginning of the semester may have to wait for up to 48 hours for their accounts to be generated. Faculty who wish to set up an eCollege account should contact Instructional Technology Services at x2756 (ckelley2@smcvt.edu), or via email at ithelp@smcvt.edu.

Getting Help
For password help, users may click on the link at the eCollege opening page: www.smcvtonline.org . For technical questions, please contact eCollege at 1-866-647-1488, or when on campus, x2022. Course-specific questions should be directed to x2756 (ckelley2@smcvt.edu), or via email to ithelp@smcvt.edu.

Knightvision

Knight Vision is a web-based application used primarily for on-line registration for classes. In addition, there are functions for supporting the faculty and staff areas. KnightVision provides students with real-time information about their class schedules, their grades and their standing in relation to degree requirements. Students can use KnightVision to look up schedules of class offerings and, during defined registration periods, to register for classes. Faculty use KnightVision to view information about their advisees, and to see their class rosters and information about course offerings. Staff member use may consist of accessing KnightVision to review budget information and leave plan information.

Access

All student, faculty and staff use requires a valid KnightVision username and password. In order to acquire a valid username and password, a Mikenet account is required. KnightVision accounts are automatically created for all undergraduate students and matriculated graduate students; adjunct and other accounts are created on request to ithelp@smcvt.edu. The point of entry for Knightvision is http://www.smcvt.edu/academics/registrar/default.asp.

Getting Help

Password help is available through the link in the lower right-hand corner of the main KnightVision page *What's my password?* – this provides the user with an option to automatically have a new password assigned and sent to an SMC email address.

Datatel

Datatel is the software used by the college for administrative purposes. Employees who need login accounts to access Datatel must complete the Datatel Account Request Form and return it to the Information Technology Department (Box C) for processing.

Access

When an account is created, the new user will also be given access to the Datatel login process through a web interface.

Getting Help

Help is provided for Datatel by the Enterprise Applications group in the Information Technology Department. Calls to the IT Helpdesk (x2020) or emails to ithelp@smcvt.edu will be routed accordingly.

Web Accounts

Two types of web accounts are available upon request:

1) Personal web: Saint Michael's College recognizes the value and potential of personal publishing on the Internet, and so allows and encourages students, faculty, and staff to design and produce personal World Wide Web pages. The views and opinions expressed in these pages are strictly those of the content authors, and comments on the contents of those pages should be directed to the author's individual E-mail address. Personalweb allows the user 4 MB of storage space. To apply, fill out the form at http://www2.smcvt.edu/itweb/forms/homepage.htm or email ithelp@smcvt.edu .

Access

The application for a personalweb account is available at http://www2.smcvt.edu/itweb/forms/homepage.htm. Once set up, your personalweb account URL will be http://personalweb.smcvt.edu/username

Getting Help

Contact ithelp@smcvt.edu for assistance with FrontPage, or get self-help from http://office.microsoft.com/en-us/training/CR061832701033.aspx . In addition, watch for faculty workshops on this application throughout the year.

2) Academic web:
Although many of our faculty uses eCollege, we also offer the option of a web site that can be used for academic purposes, whether as a standalone site or as a graphics-rich supplement to an eCollege course. Academic web sites should be directly tied to a course, a discipline, or academic research.

Access
To set up an academic web account, contact ithelp@smcvt.edu or call x2020. Once set up, your academicweb account URL will be http://academicweb.smcvt.edu/username .

Getting Help
Contact ithelp@smcvt.edu for assistance with FrontPage, or get self-help from http://office.microsoft.com/en-us/training/CR061832701033.aspx . In addition, watch for faculty workshops on this application throughout the year.

For further information about accounts at Saint Michaels College, please contact the Help Desk at 654-2020.

Mikenet Password Rules

Do I absolutely have to change my password?

Due to security reasons, all Mikenet users are required to change their passwords every 120 days. This password change does **not** impact the user's eCollege, KnightVision, or Datatel passwords.

How will I know when my password is due to expire?

When your password is due to expire, you will receive a prompt to change your password at login (either while logging into a college-owned computer or logging into email through Outlook Web Access). Follow the on-screen prompts to change your password.

Special Note for Outlook Web Access users: There are two possibilities for changing your password through Outlook Web Access (webmail). Please read the screen carefully!

Option 1. If you are changing your password ***because you were prompted to do so***, type your username as requested in the form of *Mikenet/username (e.g.: Mikenet/jdoe).* (If you have trouble resetting your password at the prompt, you may log in with your current password and then use the Options button (#2) to change your password.)

Option 2. If you are using the *Options* button through Outlook Webmail's Internet Service Manager to change your password, enter the domain name (Mikenet) on the first line, and your username on the second line. Enter your current password, your new password, and the new password a second time to confirm. Click OK and your password will be changed.

What rules do I have to follow when changing my password?

- Passwords must be at least 6 characters long and no more than 28 characters
  - Passwords cannot contain all or part of your Mikenet name or full name
  - You cannot reuse your last 3 passwords; simply changing the case of one or more letters doesn't satisfy this rule (Password1 is viewed the same as PASSword1)

- Your password must contain characters from at least **3 of the 4** categories listed here:
    1. Uppercase letters (A through Z)
    2. Lowercase letters (a through z)
    3. Numeric characters (0 through 9)
    4. Special (!@#$%^&*()_+) character

How can I pick a password that I'll be able to remember, yet follow all those rules?

Try creating a pass-phrase based password:

1. Think of a sentence that you can remember, such as *my son Adam is three years older than my daughter Anna*. This will be your pass-phrase.
2. Take the first letter of each word of the sentence to create a new word. Using the example above, you'd get: *msaityotmda*.
3. Then mix it up by using a combination of upper and lowercase letters and numbers. Example: *MsAi3yotmdA*
4. Finally, substitute some special characters that look like letters, to make this password even stronger. These tricks finish the example password to read ***M$8ni3y0tmd@***

(If you're worried about remembering your pass-phrase, start with a common phrase, such as *You can't teach an old dog new tricks*, then inject at least one number or symbol into the password. In this case, *yctaodnt* can become *YctaODnT*, or even ***U(t@0DnT***.)

How can I be sure that my password is strong enough?

Check the strength of your password at:
http://www.microsoft.com/athome/security/privacy/password_checker.mspx

Where can I get help if I'm unable to change my password?

To report problems, please either call or stop by the Helpdesk, as we are unable to change passwords via email. When calling the Helpdesk for a password-related problem, please be prepared to give your SMC ID# , which you'll find on the front of your ID card. Our Helpdesk staff is required to have this number before a password can be reset. ***Please note*** that passwords can only be reset during normal IT Helpdesk hours: Monday-Friday between 8:00AM and 5:00PM.

Email

Saint Michael's College provides an email mailbox for all faculty, staff and students through our Microsoft Exchange server. All SMC email and attachments are scanned for viruses (both inbound and outbound) and potential spam. In order to protect campus equipment, as well as personal computers, from virus attacks, users are strongly encouraged to use their Saint Michael's email account exclusively.

Our on-campus email client is Microsoft Outlook. Microsoft Outlook is part of the Microsoft Office suite and is installed on all College-owned computers. Users can access email by clicking on the Microsoft Office Outlook icon on the desktop.

Email is also available on the web through Microsoft Outlook Web Access (OWA) at https://smcmail.smcvt.edu. Mikenet users have access to their mailboxes from anywhere in the world through OWA. To get started using OWA:

1. Type the following URL into your web browser: https://smcmail.smcvt.edu
2. When prompted to Log On, enter your Mikenet username.
3. You will then be prompted to enter your username once again along with your password (be sure to press the tab key after your username to get to the password entry field).
4. When you're finished, Log Off. You'll find the Log Off icon in the Outlook task window on the left.

Spam Filtering

The College uses an appliance called Barracuda Spam Firewall to filter incoming email for spam. Over 90% of all incoming email is blocked by Barracuda. Suspected spam is quarantined. Email messages will be checked by Barracuda when they arrive and directed to your mailbox or to a quarantined area, based on a spam score value. You will receive a daily Spam Quarantine Summary email containing a list of all messages Barracuda has quarantined, for you, for that day. The list presented in the email will allow you to manage your quarantined messages and determine what you want to classify as spam. This won't impact your "normal" mail. Over time, depending on how you manage your spam filters, you should see a marked decrease in spam and have fewer summary emails to review. Resources on the web:

Barracuda Quickstart
Barracuda Spam Firewall User Guide

Public Folders

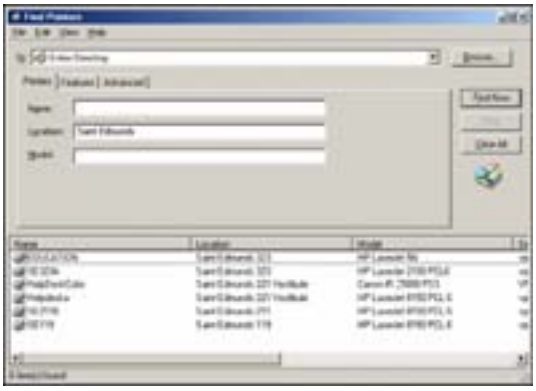
Public folders give Saint Michael's students, staff and faculty a place to organize and share information. Information in public folders is accessible only to users of Mikenet computer community. The link for "Public Folders" on the Outlook shortcut bar and Outlook Web Access allows you to view the items in the public folders.

Network Printing

Campus networked printers include printers in public labs, as well as those designated for administrative use in various departments. Our network printers are covered by a lease with Ikon. Service and supplies are obtained by calling the 800 numbers listed on the Ikon tag affixed to the printer. Each network printer has an identifying label with its network name. Printers are named by their location (*Example: JE140A = Jeanmarie Hall Room 140 – printer A)*

To add a new network printer… In order to use a network printer, you must first add it. You may connect to more than one network printer (when you want to print, simply choose from one of your connected printers). Follow the directions below to add a printer.

1. Click on the **Start** button
2. Select **Search**
3. Click on **Find Printers**
4. To find a printer that is near your location type the building name in the **Location** field and then click on the **Find Now** button
5. Double click on the printer you would like to add. When the search window disappears your printer has been added



To change your default printer…

1. Click on the **Start** button
2. Select **Settings**
3. Click on **Printers and Faxes**.
4. RIGHT click on the printer that you want to be your default printer
5. Left click on the **Set as Default Printer** option

Wireless Network Access

The wireless network provides full access to the college network (MIKENET); all users accessing the student wireless network are required to login to MIKENET. **Note: only 802.11b and g technology is supported for this network.**

Wireless hot spots are available on campus in the following locations:

- Alliot
- Cheray Science
- Durick Library
- Hoehl Welcome Center
- International Commons
- Jeanmarie Hall
- Saint Edmund's Hall classrooms & lobby
- Sutton Fire House
- Tarrant Hall of Fame Room and Field House

Wireless access points come in a variety of brands and features today. IT does not recommend any particular brand or provide support for private wireless access points. Students who install wireless access points are responsible for operating their private wireless access point in a way that does not interfere with the operation of the College's wired and wireless networks. Access points that are suspected to be a source of interference or disruptive activity on the network will be immediately disconnected.

The following rules apply for personal wireless access points:

- **Only access points or hubs are allowed**; wireless routers are not allowed because they have the possibility of disrupting the campus network.
- **Only one access point** can be installed in a room or suite
- Access points must be **configured to use DHCP**
- Access points need **a unique SSID**; you may not use any Saint Michael's SSID's
- Access points need to be **configured to use WEP** or better encryption
- Access points may be used in **student rooms and suites only**; do not connect access points to any academic or administrative locations
- The Ethernet cable that connects to the room data jack is connected to the access point.

Best Practices – Data Storage

Introduction and Purpose of Document

During the summer of 2006, IT added a considerable amount of new storage volume on the Storage Area Network (SAN) to allow for the saving of data on network drives by members of the Saint Michael's community. Space was added in three general areas:

- Profile directories (User Profiles)
- User Home Directories
- File shares

The addition of the space is intended to address the following challenges:

1. User profile size, and the effect on logon timing.
2. User need for saving and accessing data from different Mikenet systems.
3. User need for saving data in a secure space.
4. Business Continuity and Disaster recovery (BCDR).
5. Data management.

The purpose of this document is to help faculty and staff of Saint Michaels College understand the uses of the added storage space. This document will be limited to describing the different network storage spaces and give recommendations as to where specific information should be saved.

The Storage Area Network (SAN)

The network SAN is divided into several blocks of disk space called ***arrays***. The arrays can be subdivided into storage partitions for managing data. As mentioned above, certain areas of the SAN have been defined specifically for **User Profiles**, **User Home Directories**, and **File Shares**. All User Profiles (faculty, staff, and students) share a common storage area. User Home Directories have been divided into two spaces: one for all students and one for faculty and staff of the college. File Shares are divided into two main areas: Academic and Administrative. User Profiles and Home Directories will have space/growth limitations. The specific size of an individual user's Home Directory folder tree (regardless of whether it is a student, faculty or staff member) will have a maximum size potential. The File Shares, however, will be virtually unlimited in size.

Mikenet users currently have the following data storage devices available:

- Local storage on a stand-alone computer's hard disks
- CDs (external device)
- Floppies (external device)
- Flash drives (external device)
- Network storage in profiles, home directories and file shares.

What's On The Horizon

Because space limitations will eventually be in place, it will become more important for users to understand how to manage their files. In the future, it will not be possible to save huge files in profiles, nor will it be possible to use home directories as repositories for huge amounts of data.

Recommended Storage Guide

The following recommendations a guide for where specific information might be saved and stored.

Personal, non-SMC documents and files	Local Storage – hard drive or external device
Music, pictures, large non-SMC related files	Local Storage –hard drive or external device
Personal SMC files and information	Network Storage (O: or Z:)
Department files and business	Network Storage (O: or Z:)
Course information to be shared with students,	Network Storage (O:) or eCollege

colleagues	

Network storage locations should be used for all college-related files, including files that a faculty member may view as personal, but that will be used, for example, in a course or for publication. By storing files of this type on the network, their recovery is assured in case of a disaster, since all network storage devices are backed up to tape every night. (Local drives are only backed up if a user takes the time to do so.) Additionally, network storage spaces are set up with strong security and access control systems.

The O: Drive

The O: drive, is divided into two areas; ***Academics*** and ***Administrative.*** While students, faculty, and staff all have access to the O: drive, they have very different security settings.

The ***Academics*** folder is used for files and information that are to be used in classes and/or shared with students or colleagues. *College business-related information should not be stored in the Academics folder*, because students have access to this portion of the O: drive and security enforcement is more relaxed.

The ***Administrative*** section is for secure file storage by College business offices and college academic departments. Faculty and staff are encouraged to save personal College business-related information in the Administrative folder. Examples of information that should be saved in this section of the O: drive would include such data as student records, financial spreadsheets, business documents, papers being written for publication, and tests, unless the tests are for review by students. In general, if the information to be saved is related to the operation of any SMC department, whether academic or administrative, it should be saved in the Administrative section of the O: drive.

Not all departments have an Administrative folder structure in place at this time. If a department does not have a folder structure in the Administrative portion of the O: drive, that structure can be requested and set up by IT fairly quickly. Since many departments have historically not used network storage as it is now being recommended, local storage devices have been used for department information. The practice of storing College business on local drives does not provide for a secure, backed up, effective way to manage data that should not be lost.

Green Computing

Green computing is a way to encourage environmentally conscious use of technology. Computers are one of the fastest growing consumers of energy. Research shows that most desktop computers are not used the majority of the time that they are turned on.

By following the Green Computing tips listed below, you can help save energy and avoid environmental and financial costs.

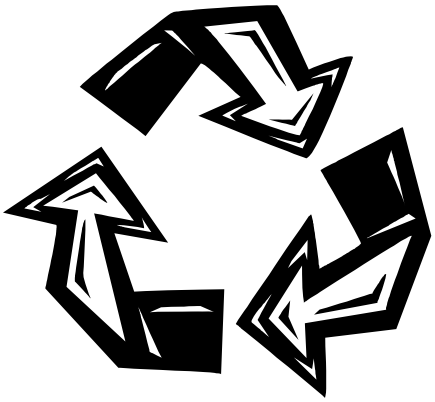
Saving Energy Tips

Tip # 1: Turn it off: Turn off monitors when they are not being used. Monitors continue to use a lot of energy even when you're not using the computer.

Tip # 2: Reduce Paper Waste: Green computing isn't just about conserving energy; we're also concerned about saving trees. Here are some ideas of how to reduce paper waste:

- ✓ Use the "Print Preview" feature to minimize hard copies that you print
- ✓ Use email whenever possible and avoid printing
- ✓ Buy recycled paper
- ✓ Print on both sides
- ✓ Pick up your print jobs – if you leave them at the printer for a long period of time, they will be recycled.

Tip # 3: Conserve: Every year over 35 million computers are thrown away. Don't throw it away. Try donating your computer to ReCycle North in Burlington, VT. Learn more about the work that they do by visiting their website: http://www.recyclenorth.org. You can also dispose of your computer at the Chittenden Solid Waste District (CSWD) for a small fee, in an environmentally sound way.



Safe Computing

Computer security is everyone's business and as cyber criminals become more sophisticated in their methods, we have to become more vigilant.

College-owned computers and Saint Michael's College email are being scanned for incoming viruses and spam. By following some of these simple practices you can reduce the risk of identity theft and infecting your personal computer.

Do's

- Delete suspicious mail without opening it.
- If the email contains an attachment, save it first so that it's scanned for a virus (don't open it).
- Keep your virus signatures up-to-date.
- Beware of an e-mail message or file attachment from someone you don't know or that seems suspicious.
- Use your SMC email so that the filters will be applied. Our server is checking for, <u>and removing</u>, infected mail.
- Be alert to downloading files from the Web. Viruses may spread when files are being downloaded from the Web. If you're not expecting a file to download, you should not accept it.

Don'ts

- Don't click on links in AIM chats or in suspect email messages.
- Don't use the AutoPreview or Preview Pane for incoming messages; using these views is the same as if you opened the email.
- Don't open mail from an unknown sender.
- Never download, open an attachment, or click on anything from an unknown source.
- Do NOT open mail from an unknown sender.

Additionally, if you receive a note you are not expecting, and it has any of the following characteristics, it may contain a virus:

- Spelling mistakes
- Errors in the message
- The sender has an obviously fake name or an anonymous handle, such as "secret admirer"
- A URL that appears odd -- e.g. www.http:// rather than http://www.

Protect your Personal Computer:

College computers receive Microsoft patches and updates automatically. The College virus protection software, eTrust AntiVirus, automatically updates with new virus signatures as they are available. You should have the same protection on your personal computer.

1. ***Use and keep antivirus software up-to-date***. If you need antivirus software for your personal computer, AVG has a free version that works well and updates itself automatically. You may obtain it by going to

   http://free.grisoft.com/doc/downloads-products/us/frt/0?prd=aff

2. ***Scan your computer for viruses.*** You can scan at any time simply by starting you anti-virus program.

3. ***Run your antispyware software on a regular basis.*** If you need an antispyware program, *Spybot Search & Destroy* is free from the web and can be downloaded at http://www.spybot.info/en/index.html. When you open *Spybot*, click on the "*Search for updates*" button. This will keep your spyware tools current and looking for the latest invaders of your PC. Click on the "Immunize" button regularly to keep spyware from recurring.

4. **Be cautious when browsing the web.** Downloads from web pages are another way to introduce viruses onto your computer. Program files and documents should always be saved to disk, virus checked and then if they appear to be safe, executed or opened. If a web site has been modified to attack your computer (as was done by the Nimda virus) the browser will pop up a window asking what you would like to do with the specified file (open, save or cancel). If you are visiting a web site are not expecting a file to be downloaded, you should cancel the operation.

Virus Protection Policy

The following is an excerpt from our full policy.
Please visit our website at www.smcvt.edu/itweb for the full text.

Objectives

The principal concern of this computer virus protection policy is effective and efficient prevention of network virus outbreaks and network security attacks involving computers associated with Saint Michael's College. Our goals are to ensure that SMC-affiliated users (faculty, staff, and students, and visitors) are aware of and take responsibility for the proper use of the College-provided and Information Technology supported virus protection software. This policy is intended to ensure:

- the integrity, reliability, and good performance of college computing resources;
- that the end user community operates according to a standard of safe computing practices;
- that the College licensed virus software is used for its intended purposes; and
- that appropriate measures are in place to reasonably assure that this policy is honored.

Policy

College approved virus protection software will be run on all Saint Michael's College computers and on all computers connected to the Saint Michael's College Network.

Goals

- Prevent all infections. And when that is not possible, create an outlet for notification and annotation of virus outbreaks for College service providers and end-users so that future breaches can be prevented.
- Prevent the loss of information/data and software on College-owned computers and minimize the cost of computing maintenance and network downtime by virus outbreaks.
- Distribute updates of virus protection software and other important campus-supported software to all College-affiliated computer users.
- Annually evaluate the number of virus outbreaks to determine whether this policy and the College-provided virus protection software are still valid and appropriate.
- Provide and continue to support the best virus protection solution that the Saint Michael's College campus can support.
- Require a minimum of end-user responsibilities in regard to computer virus protection practices.

Virus protection software is not a 100% guarantee against viruses. However, it is critical that we take every precaution that we can. Virus protection software that is not used, and updated, cannot prevent infections.

Our policies are designed to reflect current conditions. As conditions change, we will review our policies accordingly; consistent with the goals of the college and subject to the availability of financial resources.

Usage Policy for Electronic Information Systems

This document identifies the rights and responsibilities of those who use the electronic information resources at Saint Michael's College. This includes the use of academic and administrative computer systems, the networks, the on-campus information resources including telecommunications systems, and the Internet resources reached through Saint Michael's College systems.

Introduction

The electronic information systems at Saint Michael's College are provided for the purposes of instruction, research, personal development, and administration. This policy informs users of the rights they may expect and their responsibilities. This policy applies to all users of SMC system resources, including those who access these resources from off campus.

Rights

The College seeks to provide an environment in which academic usage has the first priority, and in which there is respect for freedom of inquiry and expression; opposition to censorship; privacy and confidentiality; freedom from sexual harassment; and protection of intellectual property. In particular, the same standards and principles of intellectual and academic freedom already supported by the College in other areas extend to material received through the network. This extends also to publication: the same standards of intellectual and academic freedom developed for faculty and student publication in traditional media are applicable to publication in electronic media.

In addition, respect for law, for due process, and the presumption of innocence are crucial elements of this environment.

Responsibilities

Users are expected to abide by the policies of the College, whose existence makes the use of these resources available. Every user is also expected to be considerate of the rights of other users. Examples of infringements of these principles may include, but are not limited to the following.

- Using the Saint Michael's College system for illegal or criminal purposes.
- Unauthorized use of resources for commercial enterprises.
- Substantially and willfully interfering with another person's authorized use.
- Compromising or attempting to compromise privacy or confidentiality. In particular, attempts to read another person's electronic mail or other protected files will be treated with the utmost seriousness.
- Modifying or attempting to modify system facilities without authorization, including software or hardware installation. This includes the use of the Saint Michael's College system as a staging ground to crack other systems.

- Obstructing other people's work by consuming gratuitously large amounts of system resource (e.g., network bandwidth or printers). This includes, but is not limited to, game playing or monopolizing information resources for entertainment or personal use.
- Allowing unauthorized access to accounts and passwords.
- Violating license agreements.

Individuals using College information systems resources will be held responsible for their own actions, and will be subject to local, state, and national laws, as well as Saint Michael's College policies.

Privacy and Security

Network and system administrators are expected to treat the contents of electronic files as private and confidential.

However, normal operation and maintenance of the systems requires backup and caching of data and communications, the logging of activity, and the monitoring of general usage patterns. In particular, users should be aware that public lab computers are not a private space and work should not be kept there.

In all matters relating to privacy and security of individual accounts and communications, along with requests for release of information, college personnel will abide by applicable US and Vermont laws, including the Family Educations Rights and Privacy Act or the Government Records Access and Management Act, and by existing College policies, such as are described in the Student Code of Conduct. These generally regard records as private and confidential. However, they allow for examination or disclosure of those records in response to a proper subpoena or court order from external attorneys, police, and/or administrative agencies, and in response to on-campus investigations following established College Security procedures.

Due Process: Complaints and Sanctions

Violations of the policy stated here are treated like any other Saint Michael's College policy violation, as outlined in the Student Handbook and applicable faculty and staff handbooks, and are governed by the same procedures. Notification of possible violations may be made to the Helpdesk at extension 2020 or to abuse@smcvt.edu.

In particular, the person against whom the complaint is made will be presumed innocent until proven otherwise. Nonetheless, though status should not be altered pending action on charges, system administrators are authorized to immediately take actions such as locking accounts when the safety and well-being of students, faculty, or College property is at risk. As soon as practical, the Director of Information Technology will be contacted to either authorize or suspend an investigation. The means of investigating may include, but not be limited to, monitoring traffic and files, including the contents thereof. The subject will be notified of the investigation, and of their rights, including the right to College due process, as soon as practical.

Sanctions for violating this policy can include all regular College sanctions (admonition, warning, reprimand, expulsion, etc.). In addition it can include loss of information systems access.

Open Access

The College is committed to allowing access to all electronic information sources to all members of its community, free of restrictions such as age or residency status. In particular, parents of minors should be aware than in a college setting, serving primarily adults, information resource personnel are not monitoring what their children may view, and no content filters are normally used.

Our policies are designed to reflect current conditions. As conditions change, we will review our policies accordingly; consistent with the goals of the college and subject to the availability of financial resources.

Course Applications on the Web

Access to a number of course applications is available on the web at https://smcaccess.smcvt.edu, including:

- Maple
- Mathematica
- Microsoft Project
- Minitab
- SPSS
- Ultimate Speed Reader

System Requirements:

The following system configuration has been tested and is supported by the Saint Michael's College Helpdesk:

- Windows XP with Service Pack 2
- Internet Explorer 6 or above
- The logged on user has Administrative rights to their computer

NOTE TO USERS: The Citrix system has been tested with Windows XP and Internet Explorer. MAC users may experience limited functionality when accessing Citrix applications. While other browser and/or operating system combinations may work they have not been extensively tested and are not supported at this time.

Documentation:

- Installing the Citrix Client
- Launching Applications through Citrix

Personal Computer Registration and Compliance

Computer and network security concerns have been on the increase. On campus, we have put measures in place to minimize exposure to viruses and other malicious activity. These measures consist of a three-tier approach: anti-virus protection, registration, and remediation. We use a network solution called Campus Manager to scan and register student computers on the network. In order to pass our scan, you'll need to pass each of the following checks.

1. Update Microsoft Windows with the latest patches & fixes

Windows patches and updates need to be up to date. For *Microsoft Windows XP* computers we require Service Pack 2 and the latest patches and updates; for *Microsoft Windows Vista* computers we require Service Pack 1 and the latest patches and updates.

To update *Windows*, Open Internet Explorer, select "**Tools**," select "**Windows Update**." At the Microsoft Update page, select "**Express Install**." Please update your computer on a regular basis throughout the term. You'll find additional information at http://www.windowsupdate.com

2. Make sure you have up-to-date antivirus software

To join the student network at Saint Michaels, all computers must have **one** of the following antivirus programs installed: Avast, *Eset NOD32, F-Secure, Grisoft AVG, McAfee-Enterprise, McAfee-Home, Norton or Panda.* Virus signatures should be regularly updated. Look for a button or icon in your anti-virus software to search or download updates. Be sure to update your anti-virus software before attempting to register your computer.

3. Make sure you have up-to-date anti-spyware software

One of the following anti-spyware programs must be installed in order for your computer to pass registration: *CA PestPatrol, Enigma-SpyHunter, Lavasoft-AdAware, McAfee-Home, Microsoft-Windows-Defender, Norton 360, Spybot Search And Destroy or Webroot-SpySweeper, Just as with the anti-virus signatures,* your anti-spyware signatures must also be updated. In many cases, it's as simple as starting the application and choosing the update button.

If you don't have an anti-spyware program we suggest *Spybot Search and Destroy*; download at http://www.spybot.info/en/index.html (consider a donation for the authors). When you open *Spybot*, click on the "**Search for updates**" button. This will keep your spyware tools current and looking for the latest invaders of your PC. Another tip on Spybot is to click on the "**Immunize**" button. Remember that the anti-spyware signatures should be updated on a regular basis throughout the year for your computer to continue to function smoothly.

Service Level Agreement
Student Personal Computer Support

Service Level Period: 8/22/2007 to 8/22/2008

Priority Levels for Service:

Level I: Student is unable to register machine for network/internet access.
Level II: Student machine is infected with malware.

Support Hours:

Service will be provided to the student body through the IT Helpdesk, located in Saint Edmund's 221. IT Helpdesk hours are: Monday-Friday, 8:00am-5:00pm

Requesting Service

Appointments can be made for service by calling extension 2020 or sending an email to ithelp@smcvt.edu .

Timeliness of Response

Service appointments are taken on a first come, first served basis. Appointments are scheduled in two hour blocks. Average resolution time may vary depending on the condition of the machine. Students are required to sign a liability release form as well as be present and participate during the servicing of their machine.

Escalation of Problems

Please contact the manager of the Helpdesk, at x2935.

Services and support for student owned desktop/laptop computers

Full support is provided for machines with Windows XP Professional. All other operating systems are supported on a best effort basis. We reserve the right to decline service for computers older than 4 years.

1. Assistance with machine registration and access to SMC network resources.
   a. installation of anti-virus software
   b. installation of Windows critical updates
   c. installation and configuration of anti-spyware software
2. Assistance with the removal of malware
3. Referral service to local vendors

*The IT department will **not** provide the following services:*

1. Operating system re-installation
2. Troubleshooting on computers that do not boot properly
3. Hardware installation and repair

User Responsibilities

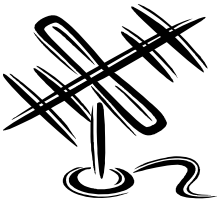
1. Students are responsible for installing and continuously updating SMC approved anti-virus software, critical system updates, and anti-spyware software.

2. Students are responsible for adhering to the Computer Usage Policy and the Virus Protection Policy, found at http://www.smcvt.edu/itweb.

This Service Level Agreement will be revisited at lease once a year prior to the opening of the fall semester.

Information Technology

SMC Cable TV Lineup



2 CBFT
3 WCAX-CBS
4 **Campus Bulletin Board**
5 WPTZ-NBC
6 TBS
7 WGMU-UPN
8 WETK-PBS
9 WLED-PBS
10 WCFE-PBS
11 **Campus Movies**
12 WVNY-ABC
13 WFFF-FOX
14 Weather Ch.
15 TNT
16 Cartoon
17 Discovery
18 Learning
19 ABC Family
20 NOAA Weather Radio
21 ESPN
22 ESPN-2
23 CNN
24 HN
25 Sci-Fi
26 E! Entertainment
27 New Eng. Sports Net.
28 ESPN Classic
29 Fox Sports New Eng.
30 Animal Planet
31 C-SPAN
32 C-SPAN2
33 MTV
34 Comedy
35 Lifetime
36 USA
37 Discovery Health
38 Game Show Network
39 A&E
40 MSNBC
41 FOX News Channel
42 History Ch.
43 Nick
44 VH-1
45 ESPNews
46 CNBC
47 MTV2
48 BET
49 Bloomberg
50 AMC
51 CSTV
52 NFL Network
53 Discovery Science
54 The Military Channel
55 F/X
56 Soap Net
57 Spike TV
58 TV Land
59 VH-1 Classic
60 WE Women's Enter.
61 AZN Television (Asian)
62 RAI (Italian)
63 RTVI (Russia)
64 TV Japan
65 TV5 France
66 TeleQuebec
67 CTV Atlantic Satellite
68 KLRA (Spanish)
69 KMCC TeleFormula
70 KUTF TeleFutura
71 **Academic Satellite**
72 Research Channel
73 **Academic Programming**
74 **Academic Programming**
75 **Academic Programming**
76 ESPNU
77 Court TV
78 G4VGTV
79 FUEL TV
80 National Geographic
81 TV ONE
82 LOGO
83 Current
84 GodTV
85 Speed
86 Reelz
87 Sleuth
88 Oxygen