

---

---

## *Computer Networking at St. Michael's College*

---

---



### **Welcome to the St. Michael's College Residence Network!**

As a new or returning resident here at St. Michael's College you have access to a *fast* connection to the Internet. This Guide is all about getting connected, staying connected, and getting the most out of your Internet connection!

The Guide is divided into four sections:

- I. Connecting and Staying Connected to the Internet.**
- II. Rules and Regulations of using the Internet.**
- III. Secure Internet/Hi-Speed Networking.**
- IV. Technical Support/Getting Help.**

Please take time to read each section **thoroughly**. It will save you time and help get you using your network connection quickly, efficiently, and safely.

If you have any questions about this document, you can send email to:  
[smc.resnet@utoronto.ca](mailto:smc.resnet@utoronto.ca)

# *Computer Networking at St. Michael's College*

## Table of Contents

### **I. Connecting and Staying Connected to the Internet**

1. Requesting Network Activation in your room.	.....	2
2. Installing your Ethernet Card and hooking up to the network.	.....	2
3. Configuring TCP/IP Networking.	.....	4
▪ Windows 95/98/ME/XP	.....	4
▪ Macintosh	.....	4
▪ Other Operating Systems	.....	5
▪ Troubleshooting and Computer Assistance	.....	5

### **II. Rules and Regulations of Using the Internet**

1. The St. Michael's College Resnet Rules and Regulations.	.....	6
2. Penalties for violations.	.....	9

### **III. Secure Internet/Hi-Speed Networking**

1. Your Responsibilities and Liabilities.	.....	10
2. How Hackers Can Gain Access to Your Computer.	.....	11
3. Securing your Internet Access.	.....	12

### **IV. Technical Support/Getting Help.**

1. Help with installing and configuring your network card.	.....	15
2. Troubleshooting your network connection.	.....	15
3. Troubleshooting your network software.	.....	17
4. Troubleshooting your email.	.....	17

## I. Connecting and Staying Connected to the Internet

Accessing the Internet through the St. Michael's College Residence Network is a little bit different from using it at home. Instead of "dialling-up" to an Internet Service Provider for access, you can now hook your computer directly to a network that has constant access to the Internet. By using the St. Michael's College Residence Network, your computer will be able to access the Internet at speeds hundreds of times faster than an ordinary telephone line.

**Connecting to the SMC Residence Network is a three-step process:**

1. Requesting Network Activation in your room.
2. Installing your Ethernet Card and hooking up to the network.
3. Configuring your networking software.

Please note that because problems often occur with older equipment, unstable operating systems, or when the necessary documentation or drivers are missing, we cannot guarantee that your particular computer will be able to connect successfully to the Residence Network. If you cannot get your computer connected, we will do our best to recommend alternative solutions.

### **1. Requesting Network Activation in your room.**

Before you can connect to the Internet through the SMC Residence Network, you must first request that the network connection in your room be *activated*. To do this please fill out the Network Activation Request Form (available from the Physical Plant Office or through the Mail Desk -- both in Elmsley Hall).

When you hand in your Network Activation Request Form you will also be asked to sign the 'St Michael's College Men's Residence Network Use Agreement', if you haven't done so already. You cannot be granted access to the Residence Network until you sign the Network Use Agreement. The terms and conditions listed in the Agreement are explained in more detail in **Section II: Rules and Regulations for Using the Internet**.

### **2. Installing your Ethernet Card and hooking up to the network.**

In order to connect to the Residence Network, you will need to acquire and install an *Ethernet card* and a *networking cable*. The Ethernet Card allows your computer to "talk" to the network directly. The networking cable connects the card you install in your computer to the network jack in your room.

## (i) Getting and Installing the Ethernet Card and Cables yourself.

(a) Getting the card. Unless your computer already has one built in as most computers do these days, the first thing you will need to do is get an Ethernet card. The Ethernet card should meet the following specifications:

- It is compatible with your computer (please consult your computer manufacturer for a list of Ethernet cards which are compatible with your model);
- It is compatible with your operating system (make sure the Ethernet card comes with all the necessary software drivers for your specific operating system, or that your operating system has built-in drivers which support it);
- It is compatible with a 10BASE-T (minimum) or 100BASE-T (recommended) network and has an RJ-45 style socket.

Even though just about any Ethernet card should work, some older cards can be very difficult to set up or may not function properly with the network, or with other parts of your computer or software. We recommend that you buy a well-known “brand name” card (such as D-Link, 3COM, SMC, Linksys, and Intel) with a PCI interface. Such cards cost between \$15 and \$40 for desktops, while cards for laptops will cost more and will have a PCMCIA (sometimes called “PC Cards”) interface. Instructions on how to install the card are usually included in a manual that comes with the card.

(b) Getting the cable. In addition to an Ethernet card, you will also need a “twisted pair” networking cable (graded “Category-5” for better performance) with RJ-45 connectors. Make sure to get a *straight-through* cable and **not** a *crossover* cable – they look the same, so be sure ask your vendor if you are uncertain. The cable should be at least 6 feet long, though a longer cable is recommended for increased convenience (i.e. getting a longer cable is easier than moving furniture).

(c) Installing the card. Unless your computer comes with the card pre-installed, the card will need to be installed. This usually means taking the cover off of your computer, inserting the card into a slot, installing software and changing operating system settings. The instructions for doing this are often included with the card. If you do not feel comfortable installing the card yourself, you can hire UofT service technicians who can do it for you. Please see **Section IV: Technical Support/Getting Help** at the end of this Guide for more information on getting help installing your card.

(d) Installing the cable. Once the Ethernet card is installed in your computer, plug one end of the network cable into the RJ-45 socket which is in the back of your Ethernet Card, and the other end into the RJ-45 socket which is in your wall. (An RJ-45 socket looks like a slightly oversized telephone jack).

## **(ii) Having the Ethernet Card and Cable installed for you.**

If you are not comfortable installing the network card and cable yourself, you can arrange to have a UofT Technician do it for you. SMC has arranged a special price on parts and labour for members of the SMC Men's Residence. Please see **Section IV: Technical Support/Getting Help** at the end of this Guide for more information on having someone set up your computer for you.

### **3. Configuring TCP/IP Networking**

Once your card is properly installed, you will need to properly configure your TCP/IP networking settings to work correctly with the SMC Resnet. How you should do this depends on your operating system.

#### **(i) For Windows 95/98/ME/XP:**

1. (If you are using Windows XP, first check to see if it has connected automatically. If it hasn't, follow these instructions.) On the Desktop, Double Click the "My Computer" Icon, then Double Click the "Control Panel" Icon to open the Control Panel.
2. Once the Control Panel is open Double Click on the "Network" Icon. Your Ethernet card should be listed under "The following network components are installed."
3. Scroll down (if necessary) and click on the "TCP/IP LAN Adapter". Click the "Properties" button. Under the IP Address tab, make sure "Obtain IP Address Automatically" is checked. Click the "OK" button. Your computer should prompt you to reboot. If it doesn't, reboot the computer. Skip to number 8.
4. If TCP/IP is **NOT** installed, click the "Add..." button on the Configuration Tab.
5. In the box labeled "Click the type of network component you want to install", highlight "Protocol" and click on the "Add..." button.
6. Under the box labeled "Manufacturer", highlight "Microsoft" and then under "Network Protocols", highlight "TCP/IP". Click on the "OK" button when you have finished.
7. If you are asked to set the TCP/IP settings, all you have to do is choose "Obtain IP Address Automatically". Click on the OK button(s), and reboot your computer.
8. After your computer has re-started, double click on the "Connect to Internet" Icon on your Desktop (if its not there, right click on the Internet Explorer Icon and choose Properties).
9. Set the connection to "Connect to the Internet using a local area network (LAN)".

#### **(ii) For the Macintosh:**

1. You must be running Open Transport to connect to the SMC Residence Network. Please install Open Transport if it is not installed already, or, if it is not available for your version of the Mac OS, upgrade your OS to version 7.5.5 or greater.

2. Go to the Control Panel menu and choose TCP/IP.
3. Select the option that says "Obtain IP Information from Server" or "DHCP Server" (the exact wording varies).
4. Close the control panel and save the setting if prompted. You are done.

**(iii) For all other Operating Systems:**

Unfortunately we are not able to advise on the proper network configurations for all the Operating Systems which are popular today. If you are using another operating system (e.g. Linux), you will have to look through your documentation or help files for instructions about how to correctly set up TCP/IP networking to work with our DHCP server.

**4. Trouble shooting and Computer Assistance**

If you are having trouble configuring your computer, or would prefer to have someone do it for you, please refer to **Section IV: Technical Support/Getting Help** at the end of this Guide for information on the various assistance options available to you.

## II. Rules and Regulations for connecting to the SMC Resnet

### **1. St Michael's College Resnet Rules and Regulations.**

As a student at the University of Toronto, please keep in mind that your network connection is provided for you primarily in support of your academic objectives and requirements. As such, there are certain Rules and Regulations which you need to be aware of when using the network at St. Michael's College (and by extension, the University of Toronto computer/data network of which it is a part). These Rules and Regulations are spelled out in detail in the "St Michael's College Men's Residence Network Use Agreement", **which you must read, and agree to** (by signing it) before you can be allowed to access the SMC Resnet. They are also summarized and explained below:

1. Because the SMC Resnet is a part of the whole University of Toronto computer/data network, you must read and agree to the University of Toronto ***Policy on the Appropriate Use of Information Technology***. This policy governs the use of all Information Technology resources in the University of Toronto and applies to all Faculty, Staff, and Students. You may ask for a copy of the ***Appropriate Use of Information Technology*** at the Information Commons located on the 1<sup>st</sup> Floor of the Robarts Library, or you can view it online at:

["http://www.utoronto.ca/ic/utordist/general/appuse.html"](http://www.utoronto.ca/ic/utordist/general/appuse.html). Please read it carefully, because abuse of this policy is treated seriously and infractions may fall under the University's Code of Student Conduct.

2. In addition to the activities listed in the University of Toronto ***Policy on the Appropriate Use of Information Technology***, inappropriate use of the College's computing and network resources may include a variety of other activities, such as the illegal distribution of copyrighted materials, the distribution or publication of offensive or objectionable materials, the unauthorized access, or attempted unauthorized access of other systems, computers, networks, etc, whether within the college or outside it, the excessive use of network resources, providing access to unauthorized users, promoting, conducting or maintaining commercial activities, transmission of unsolicited email, harassing, intimidating threatening or otherwise disrupting individuals or groups, impersonation, criminal, or other illegal activity.

3. In order to operate the Residence Network effectively, the College also reserves the right to limit the way in which students may access the SMC Resnet, and the kinds of resources they may access or provide to others through the network. In particular:

**(i) You may not manually assign an IP address to your computer.**

Just as you need a phone number in order for someone to call you, your computer needs an address on a network in order to send and receive information. An IP

(Internet Protocol) address is a unique number that specifies an “address” that your computer can be reached at on the network it is connected to. The St. Michael’s College Residence Network automatically assigns an IP number to your computer, and may change it automatically, from time to time. Manually setting this address yourself is strictly prohibited, because it impairs the smooth operation of the network. If you are unsure about how to configure the IP address of your computer, please request assistance.

**(ii) You may not connect multiple computers to your network jack.**

In each room connected to the SMC network there should be one network connection point (or jack) for each resident living there. Because you are responsible for all data transfers which come in and out of your network connection, our network hardware has a variety of security features designed to prevent other people from connecting their computers to your jack. Although this gives you added security, it also means you cannot connect multiple computers to your network jack, either through the use of ‘hubs’, ‘switches’ etc., or by “swapping” computers (i.e. connecting multiple computers to the network by unplugging the network cable and hooking it up to a different computer).

Please keep in mind that the **FIRST** computer you hook up to the network will be the **ONLY** computer that will be allowed access to the network. Any attempt to add or change computers to the network jack will result in the **SECURITY LOCKOUT** of that jack – and network access will be disabled. If you trip the lockout, please see **Section IV: Technical Support/Getting Help** at the end of this Guide for information on who to contact to have it reset.

**(iii) You may not run cable of any kind beyond your room. You may not use or share any network jack that is not located in your own designated room.**

In the past, serious damage to wall, ceiling, and carpet finishes has resulted from students attempting to connect networking cables between rooms, and often presents a trip hazard to guests, staff and residents. Stringing wires between rooms outside our buildings causes damage to window frames through bending, as well as moisture/condensation damage resulting from an improper seal during rain storms and the winter months. Therefore you should never attempt to link computers together by running wires between rooms, whether through the halls, or outside the buildings. Those who do so will have the connections removed without notice, and may be subject to fines, or charges for damage.

At no time should you attempt to use your computer in someone else’s room. Attempts to use your computer in someone else’s room will result in the **SECURITY LOCKOUT** of that jack. The attempt to use someone else’s network jack is prohibited at all times.

**(iv) You may not run DNS, DHCP/BOOTP servers, SMTP/POP/IMAP servers, or Remote Access Servers.**

St. Michael's College runs various network services that are essential to the efficient operation of a network. Attempts at running any of the above noted servers from your own computer (whether it is academically justified or not) without prior authorization is strictly prohibited. Be aware that installing or running these servers accidentally or unknowingly is **NOT** an excuse. You are responsible for your computer, and for all use of the SMC Resnet which originates from your assigned network connection point. Please read carefully the documentation that comes with your Operating System. If, when installing your Operating System, you are unsure of whether a component may violate this guideline, please contact [smc.resnet@utoronto.ca](mailto:smc.resnet@utoronto.ca) for confirmation. In the meantime, avoid installation of any components that you are unsure of.

**4.** Operating a computer connected to a network like the SMC Resnet is a little like operating a car on a public road – if you don't obey the rules of the road, or don't keep your car properly maintained, or pay attention while driving, you can injure yourself and others. On a computer network, that injury can take a variety of forms, from using so much of the system's resources that the network stops functioning properly for other users, to becoming the unwitting pawn in a hacker's attempt to injure someone else. Because of this, the St Michael's College Men's Residence Network Use Agreement requires you to acknowledge the risks and responsibilities that come with operating a computer connected to the SMC Resnet, as well as the right of the College or the University to monitor your use of the network, to limit the way you use it, and even to suspend your access to the network. This is explained in detail in the Network Use Agreement, and includes the following:

(i) You agree that you are responsible for all use of the network made through your assigned connection point (i.e. through the connection point in your room).

(ii) You acknowledge that there are risks associated with connecting a computer to the St Michael's College network, which may include loss of data, loss of service, damage to your hardware or software, violation of privacy, or other personal injury, and you agree that you are responsible for protecting your equipment and data, and that the College is not responsible if you suffer any damages or losses, howsoever caused.

(iii) You acknowledge that the College (or University) may limit your access to the network, that it has the right to monitor your network communications in order to better manage its resources and to establish compliance with the Network Use Agreement, and that inappropriate use of the College's computing or network resources may result in the suspension of your access to the network, suspension from the Men's Residence, and disciplinary action under the College's Code of Conduct. You also agree that you will be responsible for any damages that the College may suffer as a result.

**5.** You acknowledge that that College cannot guarantee that your particular system will be able to access the SMC Resnet. Acquiring the hardware and software necessary to access the network and configuring it to work with the network is wholly your responsibility.

**2. Penalties for violating the rules.**

(i) Although the limitations stipulated by the “St Michael’s College Men’s Residence Network Use Agreement” are in effect at all times in the Residence, **exceptions can be made in some cases, where there is significant academic need.** To ask for permission to carry out any activity that is prohibited by these guidelines, please contact [smc.resnet@utoronto.ca](mailto:smc.resnet@utoronto.ca) Your request will be passed on to the appropriate authorities.

(ii) **Persons who are believed to be in violation of any other part of the Network Use Agreement** will have their network connections disabled pending an investigation of the circumstances. If a violation has occurred, then depending on the nature and severity of the violation, such persons will be subject to disciplinary action which may include suspension of network access (either permanently or for a limited time), as well as disciplinary action described under the SMC Residence Agreement, the St Michael’s College Code of Conduct, the University of Toronto Code of Conduct, and criminal prosecution. A reconnection fee may also be required.

If your network connection is suspended, you may access your email account and the Internet from any of the free University of Toronto computing facilities on campus (including The Kelly Library, the Robarts Library, etc). You may also make arrangements for internet access in your room through a third party service provider, like Rogers@home, and Bell Sympatico.

**Play Safe! Play Fair!**

The SMC Resnet is here to serve all of us, and the rules are there to help everyone get the best use out of the available resources. Be responsible and considerate of others – play safe, and play fair!

### III. Secure Internet/Hi-Speed Networking

While most people are familiar with the benefits of a fast Internet connection, such as instant access to information, email, and multimedia content, far fewer people are aware of the inherent dangers associated with having such a connection.

There are two important differences between an Internet connection from home using an ordinary phone-line, and your connection to the Internet through the St. Michael's College Residence Network which you need to be aware of.

#### ❖ Network Speed

The most obvious difference between an ordinary phone-line connection and an Ethernet network connection is the data transfer speed. As has been said before, the transfer speeds in residence are potentially hundreds of times faster.

#### ❖ Always On Connection

The other difference is the fact that an Ethernet connection is 'always on'. When you are in residence, for as long as your computer is connected to the network and turned on, it is part of the Internet at large.

Fast network access and the fact that your computer is on for long periods of time makes your computer an attractive target for malicious hackers. Network connections, such as those provided through the St. Michael's College Residence Network, also give a malicious hacker a fast and stable target on which to concentrate break-attempts. While most would-be hackers may be content only to scan networks for potential targets with weak or unprotected computers, never underestimate how much harm a malicious hacker can do to your system.

#### **1. Your Responsibilities and Liabilities**

When you signed the **St Michael's College Men's Residence Network Use Agreement**, you acknowledged that there are risks associated with connecting a computer to the St Michael's College residence network, and you also agreed that the protection of your equipment and your data is your responsibility and that **St. Michael's College is not responsible for any loss or damage which you may suffer, no matter how it is caused.**

But taking responsibility for protecting your equipment and data also means taking responsibility for making sure that you and your computer will not be used by others for illegal or inappropriate activity. Unfortunately, there are many ways that computer systems damaged or used to damage other computers over the Internet:

- Damage on your own computer.

For example, just as a computer virus can damage or erase your files, or even your entire hard-drive, hackers can easily accomplish this and much more if allowed to break into your computer. Such an attacker could easily tamper with or modify your files, install computer viruses, and even steal personal information.

- Damage to other computers.

Once a hacker has compromised your machine he or she can easily set your computer up to attack other computers on the Internet. This raises several legal issues: if your computer is used to attack other computers on the Internet (even without your knowledge), you may be charged with criminal wrongdoing. If the hacker is not caught, you may have to bear the responsibilities of *their* actions! As the owner of your computer, you are responsible for ensuring that it is not used to commit any illegal or inappropriate acts.

## **2. How Hackers Can Gain Access to Your Computer.**

Hackers can compromise your system in two ways:

### **1. Compromising your computer through holes or weaknesses in the Operating System.**

Your computer's Operating System is a very complex and often large piece of software that governs how all the components in the computer work together. Because of its complexity, security weaknesses sometimes occur in the OS itself which can be exploited by hackers, either to gain access to the system, or to disrupt it altogether. Keeping up-to-date with all the software updates for your particular Operating System is an excellent habit to get into. If you use Microsoft Windows, you can download and apply security updates by going to "<http://www.windowsupdate.com>".

### **2. Tricking you into compromising your own computer.**

This is by far the most common way of gaining access to a person's computer. Either by distributing *Trojan Horse programs* or, less commonly, by exploiting scripting deficiencies in your Internet Browser, holes can be opened in the security system of your computer. A *Trojan Horse program* is a program that poses as a benign program, but in fact actually tampers maliciously with your Operating System or other programs on your computer. Most if not all *Trojan Horse programs* are distributed through Email disguised as jokes, or as seemingly harmless applications that unsuspecting people might open without thinking. Ask yourself: How often have I opened an Email attachment without really knowing exactly what it was? These *Trojan Horse programs* can do something as harmless as changing the colour of your computer desktop, to

something as malicious as permanently destroying your documents – all without the slightest sign, until its too late.

One increasingly common type of *Trojan Horse program* is designed to open security holes in your Operating System. Many of these types of *Trojan Horse programs* create access points into your computer than anyone can scan for and locate. Many of these programs can even steal your passwords automatically, watch your computer screen, or mail themselves out to your friends with your email address and a fake endorsement from you (to fool your friends into running the program and compromising their own systems as well).

**Once a hole has been established in your computer's security, it is often an easy task for anyone to break into your system.**

### **3. How to Secure your Network Access.**

The best way to defeat many of these hack attempts is to be proactive! Don't wait until it happens. Never underestimate the ways in which your computer can be compromised or damaged. Think of how much work you have at risk, as well as the legal ramifications if your computer is caught attacking other computers on the Internet!

Here are some things you can do to protect yourself:

- ◆ **Turn OFF and SECURE your computer when you are not using it.** The less your computer is on, the less chance your computer can be compromised. If your computer is only on when you are working on it, any odd behaviour will be noticed more quickly. But you should also do something to make sure that no one can use your computer without your permission. If your computer supports it, a BIOS password will go a long way toward making sure that no one can physically tamper with your computer when you're not around. Consult your computer manual on how to setup a BIOS password. If you own a Mac there should be a setting for Startup passwords in the newer versions of the MacOS.
- ◆ **Turn file sharing off.** Many Operating Systems have features which allow people to easily share files between multiple computers, either directly or through the web. But some people unwittingly leave these features turned on, or without password protection. This is a lot like leaving your car unlocked with the key in the ignition. For your own privacy and security, disable all file-sharing features in your Operating System unless you are sure you need them, and know how to configure them properly. (See the help files for your operating system for instructions).

- ◆ **Install a Virus Checker – and keep it UPDATED.** It is imperative that you have an up-to-date Virus Checker running on your system. Ask yourself how much your work is worth and you'll see that protecting it will be one of your best investments. All U of T staff and students enrolled in a degree granting program can get a free copy of Norton Antivirus from [www.antivirus.utoronto.ca](http://www.antivirus.utoronto.ca). Many commercial Virus Checkers offer free updates – make use of them on a regular basis! A Virus Checker that isn't updated is almost as bad as not having one at all. Recognize the possibility that your files are more likely to be exposed to a virus if you do work elsewhere on campus, or on a friend's computer. If any of those computers are infected, sooner or later they will infect your files and your computer too.
  
- ◆ **Install an Internet Firewall.** This kind of application blocks most of the known methods that hackers use to compromise your system through the internet. There are various personal Internet Firewalls on the market, many of which can still protect your system even if you've already been compromised! Any of the following would be useful in protecting your system:
  - Two effective Internet Firewall packages which are **free for personal use** are:
    - **Zone Alarm** - Zone Labs ("<http://www.zonelabs.com>"). (PC only)
    - **Tiny Personal Firewall** - Tiny Software ("<http://www.tinysoftware.com>") (PC only)
  
  - There are also several affordable commercial packages for PC's which might suit your needs, depending on your level of expertise and comfort: **Black Ice Defender** from Network Ice ("<http://www.netice.com>"), **Conseal Private Desktop** or **PC Firewall** from Signal 9 Solutions ("<http://www.signal9.com>"), and **Symantec Desktop Firewall** or **Norton Personal Firewall 2001** from Symantec Corporation ("<http://www.symantec.com>"), and many more.
  
  - Two good commercial products for the Macintosh are **Norton Personal Firewall for Macintosh** from Symantec ("<http://www.symantec.com>"), and **Net Barrier** from Intego ("<http://www.intego.com/netbarrier/>").
  
- ◆ **Be VIGILANT about your Email attachments.** Be VERY CAREFUL about opening Email attachments on your computer. As noted, computer Virii and *Trojan Horse programs* are spread most often by Email. If you receive an Email with an attachment that you do not recognize or did not ask for, contact the sender about it! If a stranger sends you an Email with an attachment, **don't open it**. For PCs: Be especially careful of programs with attachments ending with ".exe", ".com", ".vbs", ".scr", ".pif", or ".bat" – these indicate programs that can be *run* and which could be malicious, as opposed to files which can only be *viewed*, like pictures (e.g. files ending with ".jpg" or ".gif").
  
- ◆ **Don't share files from your computer.** Even if you know how to properly configure the file sharing features of your Operating System, you should be aware

that many popular exploits center around file-sharing on home computers. Don't share files unless you have to. If you do, unshare your files as soon as you can.

- ◆ **Don't release personal information on the Internet.** Large online companies with SECURE web servers are the lone exception to this rule. Would you give a complete stranger your name, address, and telephone number without any guarantee that your personal information will be used benignly? That's what you're doing every time you leave personal information on questionable websites.
- ◆ **Be careful when running Internet-aware applications.** Many programs which are popular today, such as over-the-Internet chat programs and file-sharing utilities (like **ICQ**, **Napster**, and Napster-clones like **BearShare** and **WinMX**) have a reputation for being less-than-secure. Try not to permit any program to allow file sharing from your computer, since this usually opens a "hole" in your system that a malicious hacker could exploit.
- ◆ **Backup your Data on a regular basis.** This can be as simple as keeping multiple copies of your work on floppy disks, or zip disks, or writable CD ROM's, or as complex as buying a RAID-enabled computer with multiple mirrored drives. Either way, a little effort will go a long way in ensuring that your work does not suffer any setbacks when things go wrong. Not only hackers, but even something as simple as power outages, a blown fuse or flipped beaker, lightning strikes, or plain old human error like a spilled cup of coffee can negatively affect your data. Make a habit of backing up your data regularly. Sooner or later, you'll be glad you did.

Following every one of these recommendations may not prevent your computer from being hacked, or save your data from being destroyed – but it will go a long way toward making sure you are not affected by any of the negative aspects of computing on the Internet.



## IV. Technical Support for the SMC Residence Network.

### **1. Help with installing and configuring your network card.**

There are a variety of support options available to help you get connected and stay connected to the SMC Resnet. But the very first step is always to complete the Network Activation Request Form and return it, along with a signed Network Use Agreement, to the Physical Plant Co-ordinator. Once the Physical Plant Co-ordinator has received your request it may take a couple of days to activate the connection point in your room (depending on how many people ask at once).

After the connection point in your room is activated, you have two installation options:

#### **(i) Full-service installation:**

If you would like to have someone install your Ethernet card for you, and configure it to work with the residence network, contact **pcservice** to arrange to have a technician come to your room and do the work for you. **pcservice** is the division of UofT Network Services which provides technical support to all UofT Departments and staff. St Michael's College has arranged a special price for members of the men's residence who would like to have their card installed for them (approx. \$60 for parts and labor, for standard installation in a pc desktop system). To request a service call please contact **pcservice** directly at **pc.service@utoronto.ca**. The technician will contact you to arrange a mutually convenient time to come by. Be sure to be in your room, or meet him or her at the front door of your building. You must pay the technician directly when he or she arrives (cash only). Be sure to confirm the price for installing a card in your particular computer before you make a booking, since prices vary for desktops, laptops, pc's and mac's. Please note that hiring a technician is a private arrangement between you and pccservice, therefore **you must pay for this service yourself**. For more information about **pcservice**, please visit their website at:

<http://www.utoronto.ca/pccservice/>

#### **(ii) Do-it-yourself installation:**

If you would like to install and configure your network card yourself (or have a technically knowledgeable friend do it for you) just follow the instructions in **Section I** of this Guide, as well as the instructions which came with your Computer, Ethernet Card and Operating System.

## **2. Troubleshooting your network connection.**

If, after carefully following the instructions in this Guide, you are still unable to connect to the SMC Resnet, follow these steps (in the order listed):

(i) Determine where the problem lies. Begin by contacting the SMC Physical Plant Coordinator to determine whether the source of the problem is the SMC Resnet or your hardware or software. This is very important. You may be unable to connect to the network because you accidentally triggered the network's 'lock-out' function, or the network may be 'down' for repair, or the connection point in your room may be damaged. If the problem is with the SMC Resnet, SMC network staff will resolve it for you.

(ii) If the problem is not with the SMC Resnet, then you have the following options:

(a) Consult the troubleshooting guides that came with your computer or network card and attempt to resolve the problem yourself;

(b) Consult the general troubleshooting guides available on the **pcservice** website (<http://www.utoronto.ca/pcservice/>) and attempt to resolve the problem yourself;

(c) Get free technical help by posting a question to the SMC Forum on the **pcservice** website (<http://www.utoronto.ca/pcservice/>). The SMC Forum is monitored by **pcservice** technicians, who will post answers to your questions as soon as possible. To access the SMC Forum you will need a special login name and password, which is available to residents through the SMC Mail Desk;

(d) Have **pcservice** staff come to your residence room for a service call. This is a private arrangement between you and **pcservice**, therefore **you must pay for this service yourself**. St Michael's College has negotiated a special price for members of the men's residence (approximately \$30/hour – which is half of the regular rate). For more information and to request a service call, please visit the **pcservice** website at (<http://www.utoronto.ca/pcservice/>) or contact the service technician directly at **pc.service@utoronto.ca**.

(e) Call a third-party service technician. Instead of calling **pcservice** you can have a different company fix your computer. But this is a private arrangement between you and the service provider, and **you must pay for this service yourself**. There are many computer technicians and repair shops in the city (some reputable, some not). Unfortunately, St Michael's College does not maintain a list of third party technicians. **pcservice** is our recommended service partner.

### **3. Troubleshooting your network software.**

The **University of Toronto Information Commons** operates a **Help Desk** which provides free technical support for a variety of UofT network services, including UTOReMail (email) and access to the World Wide Web. This includes help with the installation and use of the software recommended for accessing these services, and for other personal computing software commonly used on campus. In many cases, **Help Desk** staff will be able to answer your questions or resolve problems when you call their **Help Line (416) 978-Help (4357)**. For a full list of their services, a list of the software which they support, contact information, and on-line trouble-shooting guides, please consult their homepage at:

<http://www.utoronto.ca/welcome.html/helpdesk/index.html>

### **4. Creating and troubleshooting your UofT email account.**

If you don't have one already, you can create a free University of Toronto email account. For instructions on creating your Email account please go to the **Information Commons** on the 1st floor of Robarts Library or view the UofT Email page at "<http://www.mail.utoronto.ca>". For all inquiries about UofT Email, please visit or contact the Information Commons. Their telephone support number is (416) 978-HELP (4357).

We hope this Guide has helped you better understand the computing environment here at the St. Michael's College. If you have questions or comments about this document, please email [smc.resnet@utoronto.ca](mailto:smc.resnet@utoronto.ca).

**Happy Computing!**

---

---

Issued August, 2001. Version 1.0

Revised August 2002. Revised April 2003.

© 2001 University of St Michael's College.

The University of St Michael's College gratefully acknowledges the assistance of Shahir Al Rashid and Innis College in the development of this document.