Saint Michael's College
Computer Security Standard

1.0 Purpose

The following computer security guidelines should help protect you and your computer while you are on campus or when connecting to the Saint Michael's College network. We highly recommend following these standards because, unfortunately, computers do get virus infections, laptops get stolen, and weak passwords get exploited. Computer security problems can be a real nightmare, leading to the loss of important data (along with loss of valuable time and effort), loss of access to services, degraded or slow performance and networking, and even theft of personal information.

We recommend the following:

- Use a strong password for your user account
- Run anti-virus/anti-malware software
- Keep your computer up-to-date
- Browse safely
- Lock it up
- Back it up

2.0 Strong Password

Attackers can easily guess blank or weak system passwords to gain access to an account on your computer in person or, sometimes, over the network. You should use a strong password with a mix of both capital and lower case letters, numbers, and special characters (like '#', '@', or '$') to protect your computer. Guidelines for creating strong passwords can be found in the Saint Michael's College Password Standard.

3.0 Anti-Virus/anti-malware Software

Malicious software is always a threat, and spreads in numerous ways — web sites, downloads, attachments, flash drives, and over the network. Saint Michael's College requires that all computers and mobile devices connecting to the network have antivirus software installed. We recommend a second level support for spyware protection. The following software is approved by the College: Avast, Eset NOD32, F-Prot, F-Secure, Grisoft AVG, McAfee-Enterprise, McAfee-Home, Microsoft ForeFront, Norton EndPoint, and Panda.

4.0 Firewall

Most operating systems for desktop or laptop computers offer a firewall that allows your computer to connect to the network while limiting how others can connect to your computer. With a firewall enabled, your computer will be protected from many network-based threats and attacks. Windows-based computers will have a firewall enabled by default. Mac OS X computers have a built-in firewall program called "Firewall", but it is disabled by default and must be enabled in order to work. Mobile devices using iOS and Android do not have built-in firewalls, but firewall software can be installed if desired.

6.0 Updates

Outdated software and apps are the most commonly used attack vector for viruses and malware. Operating system updates are also critical for security, and Windows and Mac users should configure their older computer for automatic security updates whenever possible. (New Windows and Mac computers are typically configured for automatic security updates by default.) Operating system updates are also vital to keeping mobile devices working well, so don't skip this important step on your phone or tablet!

7.0 Browse Safely

By adjusting the settings in your browser you can significantly increase security while online and minimize the threat of picking up a virus or other malware from infected websites. Some browsers also allow add-ons, which give the user more control over content and how it is displayed. Be careful where you click—popup windows are frequent sources of malware. If in doubt, contact the IT department before clicking on an unsafe link. If you're on a secure site, you'll see https:// instead of http://.

8.0 Lock It Up

The security tips above all involve software threats, but you should take steps to protect your computer from real-world physical threats as well. Locking your screen when your computer is not in use should prevent any unauthorized access and help protect your privacy. (On a Windows machine, you can lock it by using the Windows key+L.) Don't leave your computer unattended anywhere on campus on in your car in order to prevent theft. For mobile devices like smart phones and laptops, consider using tracking services like "Find My iPhone" or enabling tracking to help you recover the device if it is ever stolen.

9.0 Back It Up

No matter how diligent you are about protecting your computer, problems may still arise. When protection fails, you want to have a backup of your important data from which to recover. Cloud services, your Saint Michael's College network drive space (Z:drive), external hard drives, and USB drives all make for good places to back up your data. But before you back up, consider protecting your personal data by using encryption to keep it from falling into the wrong hands. For more information about encryption, please contact the IT Helpdesk at x2020.