



5.11 INTERNET AND COMPUTER USE POLICY December 2008.

Internet & Computer Policy

- 1. Rationale**
- 2. The Internet**
 - 2.1 Student Rights**
 - 2.2 Student Responsibilities**
 - 2.3 Staff Rights**
 - 2.4 Staff Responsibilities**
- 3. Computer hardware**
- 4. Software and operating systems**
- 5. Networks**
 - 5.1 Student rights**
 - 5.2 Student responsibilities**
 - 5.3 Staff Rights**
 - 5.4 Staff Responsibilities**
- 6. Printing**
- 7. Possible penalties**

1. Rationale

As we educate our students for a rapidly changing world, we believe it is important for them to learn how to use technology constructively and responsibly.

The Internet is a global network, linking computers at universities, schools, government departments, businesses and homes. On the Internet, one can access information and communicate with people all over the world through web sites, discussion forums, as well as through electronic mail.

Use of the Internet provides many direct and indirect benefits to our students and staff. These include:

- access to vast libraries of information from sources throughout the world
- the ability to interact and collaborate with other students and knowledgeable adults
- the ability for staff to collaborate with other educators and interested parties
- the acquisition of knowledge and skills that will be useful throughout their lives
- the opportunity to publish their own material to a wide audience

As a communication medium, the Internet's potential is boundless. However, although the Internet is of significant educational value, care needs to be taken with its use in order to exploit efficiently, effectively and appropriately this potential. Due to band width considerations, internet access should be used for educational purposes, otherwise internet access may be very slow.

2. The Internet

Internet access is expensive and has been provided to assist in the education process.

Students must use it only with permission, and not in any unauthorized way. It is not intended for entertainment.

During class time, teachers are responsible for student use of the Internet. For use outside class time the Library has procedures that allow access to the Internet on an individual basis. Although supervision is provided it is acknowledged that students will at times have access to the internet without direct staff supervision.

The school recognizes its responsibility to ensure that, as far as possible, material obtained from the Internet is not offensive or inappropriate. To this end, filtering software has been placed on the Internet links. In the end, however, it is the responsibility of individual students to ensure their behaviour does not contravene college rules or rules imposed by parents/guardians.

The school recognizes its responsibility to ensure that, as far as possible, material obtained from the Internet is not offensive or inappropriate. To this end, filtering software has been placed on the Internet links. In the end, however, it is the responsibility of individual staff member to ensure their behaviour does not contravene college rules or rules imposed by society, e.g. pornography or inappropriate material.

The school is aware that no security system is perfect and that there is always the possibility of inappropriate material, intentionally and unintentionally, being obtained and displayed.

It is the responsibility of the school to:-

- provide training on the use of the Internet and make that training available to everyone
- make users aware of the School Internet Access Policy
- take action to block the further display of offensive or inappropriate material that has appeared on the Internet links

2.1 Student Rights

Students are also provided with access to the internet. Material that can be accessed on the World Wide Web is limited by blocking software in an effort to avoid students accessing material that the school deems inappropriate such as violent, pornographic, commerce, email and advertisement sites.

Students are not provided with an email account and are not permitted to access or utilize any personal email accounts while at school.

Student accounts are limited in the amount of data that can be stored. This measure has been put in place to avoid overloading the system.

There is also a limit on the amount of time that a student can spend using their account. This measure has been put in place to provide fair access to computers by all students and to avoid certain students monopolizing the computers.

2.2 Student Responsibilities

As with all resources provided by the College, the College's Internet connection is for educational purposes. The most important prerequisite for Internet use is that the student take full responsibility for her/his own actions and their effect on others. It is the student's responsibility to:

- not deliberately seek out, create or print out material that could be offensive to anyone. This includes information that is racist, sexist, pornographic, irreligious or contains abusive language
- not deliberately enter or remain in any site that has any of the following content:
 - Nudity, obscene language or sexual discussion intended to provoke a sexual response
 - Violence
 - Information on, or encouragement to commit any crime
 - Racism
 - Information on making or using weapons, booby traps, dangerous practical jokes or "revenge" methods
 - Any other material that the student's parents or guardians have forbidden them to see

If students encounter any such site, they must immediately turn off the computer monitor (not the computer itself) and notify a teacher.

Do not show your friends the site first, and do

- not post messages and attribute them to other users
- not to use email to copy information that is personally abusive to the recipient or any other person
- not interfere with, harm or destroy the computer work of any person
- not break copyright law by copying and/or redistributing another's work
- not copy the ideas of others and present them as her own (plagiarism)
- not access Internet chat for safety reasons
- refrain from excessive printing
- not reveal personal information including names, addresses and telephone numbers of themselves or others
- acknowledge appropriately downloaded material used in preparing work
- not steal, or deliberately or carelessly cause damage to any equipment
- not interfere with or change any software settings or other people's files
- not attempt to get around or reduce network security
- not do anything in any other person's home directory
- not store unauthorized types of files in their own home directories
- not use the internet for commercial purposes or for profit.
- not use the internet for be used for illegal purposes such as spreading computer viruses or distributing/receiving software that is not in the public domain.
- not act as though you intend to break the law e.g. by attempting to guess a password or trying to gain unauthorized access to remote computers. Even if such attempts are not seriously intended to succeed, they will be considered serious offences.

These requirements are displayed near all computers that provide Internet access. Failure to observe them will result in loss of Internet access at the College.

2.3 Staff Rights

Staff are also provided with access to the internet. Material that can be accessed on the World Wide Web is limited by blocking software in an effort to avoid students accessing material that the school deems inappropriate such as violent, pornographic, commerce, email and advertisement sites.

Staff are provided with an email account and are permitted to access or utilize any personal email accounts while at school.

2.4. Staff Responsibilities

As with all resources provided by the College, the College's Internet connection is for educational purposes. The most important prerequisite for Internet use is that staff take full responsibility for their actions.

It is the staff's responsibility to:

- not deliberately seek out, create or print out material that could be offensive to anyone. This includes information that is racist, sexist, pornographic, irreligious or contains abusive language
- not deliberately enter or remain in any site that has any of the following content:
 - Nudity, obscene language or sexual discussion intended to provoke a sexual response
 - Violence
 - Information on, or encouragement to commit any crime
 - Racism
 - Information on making or using weapons, booby traps, dangerous practical jokes or "revenge" methods
 - Any other material that the student's parents or guardians have forbidden them to see

If staff encounter any such site, they must immediately notify the college of the web site so it can be blocked.

Do not show other staff the site first, and do

- not post messages and attribute them to other users
- not to use email to copy information that is personally abusive to the recipient or any other person
- not interfere with, harm or destroy the computer work of any person or the College
- not break copyright law by copying and/or redistributing another's work
- not reveal personal information including names, addresses and telephone numbers of students or others
- acknowledge appropriately downloaded material used in preparing work
- not steal, or deliberately or carelessly cause damage to any equipment
- not interfere with or change any software settings or other people's files
- not attempt to get around or reduce network security
- not do anything in any other person's home directory
- not store unauthorized types of files in their own home directories

- not use the internet for commercial purposes or for profit.
- not use the internet for be used for illegal purposes such as spreading computer viruses or distributing/receiving software that is not in the public domain.
- not act as though you intend to break the law e.g. by attempting to guess a password or trying to gain unauthorized access to remote computers. Even if such attempts are not seriously intended to succeed, they will be considered serious offences.

Failure to observe these requirements could result in loss of Internet access at the College.

3. Computer hardware

Computer facilities are expensive, sensitive and must be treated carefully.

Staff and Students must not:

- Do anything likely to cause damage to any equipment, whether deliberately or carelessly
- Steal equipment
- Vandalize equipment (e.g. graffiti)
- Mark or deface any equipment
- Interfere with networking equipment such as hubs
- Eat or drink near any College owned computer resources

Staff and Students must not, without permission:

- Attempt to repair equipment
- Unplug cables or equipment
- Move equipment to another place
- Remove any covers or panels
- Disassemble any equipment
- Disable the operation of any equipment

Staff and Students must report other people breaking these rules.

Regardless of the real or supposed levels of understanding, staff or students are NOT authorized to attempt the repair or adjustment of any college hardware or software. Any such attempt will be regarded as a violation of network security. Any problem with equipment or software must be referred to an authorized person.

4. Software and operating systems

Computer operating systems and other software must be set up properly for computers to be useful. Students and Staff will not:

- Change any computer settings (including screen savers, wallpapers, desktops, menus standard document settings etc) without permission
- Bring or download unauthorized programs, including games, to the college or run them on college computers. Online internet games are banned.
- Delete, add or alter any configuration files
- Copy any copyrighted software to or from any computer, or duplicate such software
- Deliberately introduce any virus or program that reduces system security or effectiveness

5. Networks

5.1 Student rights

- Students are provided with a password protected computer account on which they can access school provided programs and store appropriate educational material.
- Student accounts are limited in the amount of data that can be stored. This measure has been put in place to avoid overloading the system.
- There is also a limit on the amount of time that a student can spend using their account. This measure has been put in place to provide fair access to computers by all students and to avoid certain students monopolizing the computers.

5.2 Student responsibilities

- Network accounts are to be used only by the authorized owner of the account. If a student finds a computer logged in, he or she should do nothing in that account except log out.
- It is the responsibility of students to make backup copies of their work. The college will exercise due care with backups but will not be held responsible for lost data.

Students must not:

- Attempt to log into the network with any user name or password that is not their own, or change any other person's password
- Reveal their password to anyone except the system administrator or classroom teachers, if necessary. Students are responsible for everything done using their accounts, and everything in their home directories. Since passwords must be kept secret, no user may claim that another person entered their home directory and did anything to cause college rules to be broken.
- Use or possess any program designed to reduce network security
- Enter any other person's home directory or do anything whatsoever to any other person's files
- Attempt to alter any person's access rights
- Store the following types of files in their home directory, without permission from the Computer Systems Manager:
 - Picture files, unless they are required by a subject
 - Obscene material – pictures or text
 - Obscene filenames
 - Insulting material
 - Password-protected files
 - Copyrighted material
- Intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users.

The School has the right to examine disks, USB sticks or other storage devices in students' possession if it is felt they might contain unacceptable material.

5.3 Staff rights

- Staff are provided with a password protected computer account on which they can access school provided programs and store appropriate educational material.

5.4 Staff responsibilities

- Network accounts are to be used only by the authorized owner of the account. If a staff member finds a computer logged in, he or she should do nothing in that account except log out.
- It is the responsibility of staff members to make backup copies of their work. The college will exercise due care with backups but will not be held responsible for lost data.

Staff must not:

- Attempt to log into the network with any user name or password that is not their own, or change any other person's password
- Use or possess any program designed to reduce network security
- Enter any other person's home directory or do anything whatsoever to any other person's files
- Attempt to alter any person's access rights
- Store the following types of files in their home directory, without permission from the Computer Systems Manager:
 - Picture files, unless they are required by the school, e.g. School
 - Obscene material – pictures or text
 - Obscene filenames
 - Insulting material
 - Password-protected files
 - Intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users.

6. Printing

Students must minimize printing at all times by print previewing, editing on screen rather than on printouts and spell-checking before printing.

Students must not load paper into printers without permission. Paper that is pre-used, torn, creased, damp, irregularly shaped or sized or unsuitable for laser printers should not be used in laser printers.

Printing is allowed in the library at a cost of 10 cents per page. Printing is allowed in the computer room at the discretion of the teacher supervising the class.

7. Possible penalties for Students:

More than one may apply for a given offence. Serious or repeated offences will result in stronger penalties.

- Ban on lunchtime computer use
- Temporary ban on using computers
- Removal of internet access privileges

- Removal of home directory and network access
- Detention
- Paying to replace damaged equipment
- Removal from classes where computer use is involved
- Suspension from College
- Criminal charges may be laid with the police

The following section needs to be filled in by the student and his/her parents or legal guardian before internet access is allowed.



ACCEPTABLE USAGE POLICY FOR STUDENTS

FOR THE USE OF COLLEGE LEARNING TECHNOLOGY RESOURCES

Before you may use computer facilities at St Mary's Coptic Orthodox College, you must sign this contract which binds you to the following conditions. If you break any of the conditions, appropriate penalties will be applied.

Your name: _____ **Form:** _____

Network login name: _____

I have read the Computer and Internet usage policy document and agree to obey the guidelines and conditions in it.

Signed: _____

Date: _____

This section must be completed by the parent or legal guardian of the student

I, the parent or guardian of _____ have read and understand the Computer and Internet usage policy document. I agree that my child shall observe these guidelines and conditions.

Name of parent or legal guardian: _____

Signature of parent or legal guardian: _____

Date: _____

Document No:	5.11
Drafted by	SMCOC
Date of Acceptance	
Review Date:	
Minor Review Date:	December, 2008
