CLAREMONT McKENNA COLLEGE

Policy Library

Volume X:	Information Technology Services
Chapter E-Mail:	Anti-Virus Policy
Approved by:	Administrative Computing Committee (ACC)
History:	Issued: 09/25/2001 Revised: 12/20/2006 Reformatted/Revised: 12/14/2009
Related Polices:	Acceptable E-Mail Usage, Configuration of Out-of-Office Message, E-Mail Distribution Lists, E-Mail Signature Block Standard, Submitting Mass E-Mails to Claremont McKenna College
Additional References:	N/A
Responsible Official:	Office of Information Technology Services

I. POLICY STATEMENT

- To ensure that Claremont McKenna College computing resources are protected by proper use of anti-virus software and computing practices.

II. ENTITIES COVERED BY THIS POLICY

- This policy covers students, faculty, staff, alumni, and research use of Claremont McKenna College computing resources.

III. CONTACTS

Direct any questions about this policy to your department's supervisor. Questions about specific issues may be addressed to:

Subject	Contact	Telephone[1]
Anti-Virus Policy	Chief Technology Officer	71553

IV. DEFINITIONS

- Also included is a list of common sense tips on reducing the chances of getting a computer virus. This is not an exhaustive list. The most important thing to remember is to use your common sense.

[1] Numbers refer to on-campus extensions. When calling from an off-campus line, please dial (909) 62+extention for numbers beginning with a "1" and please dial (909) 60+ extension for numbers beginning with a "7."

V. DETAILS

- Students who wish to connect their computers to CMC networking resources are required to use antivirus software on the approved list that is updated yearly by ITS and enforced by the Student Technician Assistant Team. Faculty and Staff using CMC computers will use anti-virus software that will be installed by ITS. Faculty and Staff not using CMC computers (either on campus or offcampus when using VPN) will be responsible to ensure that they have anti-virus software with current anti-virus signatures running on their computer(s). ITS reserves the right to deny CMC faculty and staff from connecting non-CMC equipment to CMC networking resources. All CMC community members using IT resources are advised to take proper precautions. The following are tips on helping to prevent viruses:

    - Do not open any files attached to e-mail unless you know what it is, even if it appears to come from a friend or someone you know.

    - Do not open any files attached to e-mail if the subject line is questionable or unexpected.

    - Before you open an attachment, it is best to save the file to your hard drive to allow your anti-virus software to examine the file before opening the file in the application by just double clicking on it.

    - Do not open any files attached to e-mail from an unknown, suspicious or untrustworthy source.

    - Delete chain e-mails and junk e-mail. Do not forward or reply to any of them. These types of e-mail are considered spam, which is unsolicited, intrusive mail that clogs up the network.

    - If you receive email containing virus warnings, please forward them to ITS for review before forwarding them to others. Many virus warnings that users receive are actually hoaxes. Some have even tried to convince users to delete files (claimed to be the virus) from their systems, where the files were actually necessary parts of the operating system.

    - Do not download any files from strangers. Do not download programs from the internet and install them on your computer if you are using a CMC computer. All software installed on CMC computers must be installed by ITS.

    - Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one.

    - Verify your anti-virus software is updating automatically. Innumerable viruses are discovered each month, so you'll want to be protected. You may also need to update the product's scanning engine as well.