MEMORANDUM

TO: All Locations

FROM: Information Technology Services (ITS)

SUBJECT: **** CRITICAL** VIRUS/WORM THREAT**

ITS has identified the presence of a "replicating virus/worm" threat that is appearing within the school site networks of the MDCPS Network community. This worm is not necessarily transmitted via e-mail, but instead is a "PC to PC" type of attack. The effect of this worm is massive network traffic that is being transmitted from school site to school site. In order to maintain a reliable level of network operability, ITS will be scanning school site networks and **shutting down** those sites that have been infected by this worm. Shutting down means denying access from the school site to the Internet until the local site tech(s) corrects the situation. If the infection persists, your router will go into a Denial Of Service attack which will result in the loss of access to CICS applications, Intranet applications, and District E-mail.

To prevent your site from becoming infected, it is critical that the steps below are followed:

1. Keep ALL site computers turned on 24/7.
2. Set all computers to "automatically update" Microsoft Operating System patches.
3. Insure that **ALL** computers have McAfee EPO client software installed and functioning.

IMPORTANT NOTE: Secondary schools that use the Mac School Scheduler will be unable to run Mac School Transfers (Quickeys) if the school site is shutdown.

Your cooperation is greatly appreciated. If you have any questions regarding this memo, please call Support Services at 305-995-3705(0).