MEMORANDUM

TO: All Locations

FROM: Information Technology Services (ITS)

SUBJECT: **INTERNET/INTRANET ACCESS**

The District is experiencing a serious virus attack threat. The effect of this virus is creating massive network traffic that is causing problems with access to the Internet and Intranet applications (ex: Winsurf, WISE, and SPI). In addition, because Passport goes through the Wide Area Network (WAN) users may experience problems accessing CICS.

Due to the nature of this computer virus, Information Technology Services must take action to secure the District computer environment. If a site is found infected, the District will take steps to prevent the spread of the virus to other school sites; which means no District Internet access. Technical staff in the school/location should ensure that all computers are left on 24/7 and are set to automatically update Microsoft Operating System patches. Most importantly, your site must have the McAfee EPO client software installed and functioning on all computers.

To prevent the spread of the virus, the following steps should be taken at schools:

- School technicians should set all Windows NT, XP and 2000 machines to perform “Auto Updating” of patches. A review of District equipment has found many machines in a **vulnerable** state due to system updates not being regularly performed.
- The default time for auto updating by Microsoft is scheduled for 3:00 am each night. To ensure this time slot is available, technicians should change the default time.
- All machines should be turned on and left on until further notice. Power saving systems (i.e. Johnson) in schools may continue to function as designed.
- Principals and technicians should make every attempt to implement the District’s anti-virus solution, McAfee EPO. If implemented and if your location schedules regular system updates, you should be protected from further outbreaks.
- Non-permanently connected laptops that may have been connected elsewhere (i.e. the WISE application machines) should not be connected to any site unless the machine is scanned with a virus protection tool.

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