

Pittsburgh Public Schools
Virus Protection Guidelines for User Accounts
May 25, 2005

These guidelines are intended for use by all authorized account owners who have been provided user accounts by the School District of Pittsburgh to prevent virus problems.

Do:

- always check your computer virus definitions and insure they are up-to-date (no more than 1 week old). Most systems in the District perform this update process automatically, but checking it manually will help insure your data is fully protected.
- always log off, but don't shut down your computer when you leave at night so that the virus update process can occur overnight. Monitors should be turned off.
- always scan a floppy diskette from an unknown source for viruses before using it.
- avoid direct disk sharing with read/write access unless there is an absolute business requirement to do so.
- utilize local drives such as CD burners to back-up your critical data on a regular basis and store the data in a safe place.
- delete spam, chain, and other junk email without forwarding.

NEVER:

- attach any system to the District network which doesn't contain an updated virus protection application as per the District's *Acceptable Use Policy*.
- open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately!
- download files from unknown or suspicious sources.