



THE PATHWAYS SCHOOLS COMPUTER SECURITY PROCEDURES

The Pathways Schools computers are set up with security features to protect both the school and individual users. These features include the password protected user accounts of Staff, Student, and Tech Support; password protected email accounts; and other security focused programs to protect from viruses, adware and spyware, as well as, internet filtering software.

The password protected user accounts are designed for use by the three types of computer users. It is very important that the accounts are accessed by the correct type of user. Below are descriptions of the accounts and some guidelines for their use:

STAFF: The Staff Account is for staff member users only. This account is set up as a Computer Administrator and has full rights to install and remove hardware, add and delete software programs; change passwords to the User Accounts and other password protected programs (i.e. CyberSitter, etc.). It has rights to perform any updates needed to keep the operating system current (i.e. Norton Antivirus and Windows XP).

STUDENT: The Student Account is for student users only. This account is set up as Limited account and only has the right to change its own password.

TECH SUPPORT: The Tech Support Account is for use by technical support staff only. This account is set up as a Computer Administrator and serves as the account from which the computer is maintained during Monthly Maintenance and /or emergency visits.

GUIDELINES FOR APPROPRIATE USE OF STAFF ACCOUNT

➤ **Log Off The Computer:**

When leaving a computer staff should Log Off by:

Clicking the **START** button – **Log Off** – **Switch Users**. This allows running programs and files to remain open while away from the computer. This action will return the computer back to the login screen and effectively **locks** unauthorized users out of the Staff account.

Benefits of Logging Off:

- Prevents students getting to a computer and changing the User Account passwords or downloading and installing programs, many of which, are actually adware or spyware, with potentially harmful effects to the computer.
- Prevents students from viewing, printing, or sending confidential documents and / or emails from a Pathways Schools email account. *NOTE: This is especially important since Pathways is responsible for every email that goes out regardless of who sent it. Individual users of The Pathways Schools computer services are responsible for their use of this resource. (See The Pathways Schools Acceptable Use Policy For Staff Using The Internet for more details).*

GUIDELINES FOR APPROPRIATE USE OF THE STUDENT ACCOUNT

- Researching classroom projects;
- Utilizing the software based learning programs available as part of school curriculum;
- Finding exciting new information on the internet;
- Communicating with other students and educators about issues relevant to and consistent with the academic curriculum of the Pathways Schools.

Failure to follow these guidelines can result in improper use of e-mail by unauthorized users, inappropriate access to confidential and sensitive information, and/or serious damage caused by inappropriate installation of virus and/or adware related software.