



Data Backup and Anti-Virus Policy

Created Sep 2006 – Updated March 2012

1. INTRODUCTION

This policy needs to be read in conjunction with the following school policies: ICT, E-Safety.

2. AIMS AND OBJECTIVES

- To ensure the efficient running of all computerised admin systems
- To reduce the threat from spyware
- To reduce the threat from viruses
- To ensure that the school has an efficient and reliable system for backing up important data

3. DEFINITIONS

- **What is a virus**
 - A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.
 - Since 1987, when a virus infected ARPANET, a large network used by the Defense Department and many universities, many antivirus programs have become available. These programs periodically check your computer system for the best-known types of viruses.
 - Some people distinguish between general viruses and *worms*. A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.
- **What is spyware**
 - **(n.)** Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.
 - Spyware is similar to a Trojan horse in that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.
 - Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.
 - Because spyware exists as independent executable programs, they have the ability to monitor keystrokes, scan files on the hard drive, snoop other applications, such as chat programs or word processors, install other spyware programs, read cookies, change the default home page on the Web browser, consistently relaying this information back to the spyware author who will either use it for advertising/marketing purposes or sell the information to another party.



Data Backup and Anti-Virus Policy

Created Sep 2006 – Updated March 2012

4. THE ROLE OF GOVERNORS

- The governing body has a duty to monitor personnel and financial matters in school. To do this it has to have up to date information. Therefore the governing body at Molescroft Primary School have a role in making sure that effective anti virus, anti spyware and backup procedures are in place.

5. THE ROLE OF THE HEAD TEACHER

- To ensure that the appropriate anti virus, anti spyware and backup procedures are in place.

6. THE ROLE OF THE ICT COORDINATOR

- To ensure that the anti virus / spyware and backup procedures are working, appropriate and meet the needs of the school.

6 MONITORING AND REVIEW

- This policy will be reviewed annually
- The SMT will monitor the effectiveness of this policy



Data Backup and Anti-Virus Policy

Created Sep 2006 – Updated March 2012

7 PROCEDURES

AntiVirus / Spyware

- All Personal Computers running any windows operating system must have Microsoft Security Essentials installed and set to run automatically each day.

Back Ups

- The following data is to be backed up daily
 - SDrive (Admin Data / Sims)
- The following data is to be backed up weekly
 - OSX Server

Backing Up S Drive

The main Admin machine has been set up to do a backup of the WP, XL and sims directory each evening. The backup files are put into a folder called mon backup on the desk top.

The above are shared folders on the Packard Bell 250 GB removable Hard drive. This will be taken home each night by an Admin Officer.

This means that there should always be a backup available that is less than a week old.

Backing Up OSX Server

This back-up contains children's work and is automated. The back up is made onto a separate HD within the server.