



Admin Data Backup and Anti- Virus Policy

Created on 11/9/2006 Reviewed September 2010

1. INTRODUCTION

This policy needs to be read in conjunction with the following school policies: ICT, Data Protection and Internet 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.



Admin Data Backup and Anti- Virus Policy

Created on 11/9/2006 Reviewed September 2010

- 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.
- Licensing agreements that accompany software downloads sometimes warn the user that a spyware program will be installed along with the requested software, but the licensing agreements may not always be read completely because the notice of a spyware installation is often couched in obtuse, hard-to-read legal disclaimers.

• What is backing up

- (v.) To copy files to a second medium (a disk or tape) as a precaution in case the first medium fails. One of the cardinal rules in using computers is back up your files regularly.
- Even the most reliable computer is apt to break down eventually. Many professionals recommend that you make two, or even three, backups of all your files. To be especially safe, you should keep one backup in a different location from the others.

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, anti spyware and backup procedures are working, appropriate and meet the needs of the school.



Admin Data Backup and Anti- Virus Policy

Created on 11/9/2006 Reviewed September 2010

6 MONITORING AND REVIEW

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

7 PROCEDURES

SPYWARE

- All Personal Computers running any windows operating system must have adaware anti-spyware installed
- The software is to be run at least once a week by the main user of the machine (teacher or administrative officer). *See Appendix 1*

ANTIVIRUS

- All Personal Computers running any windows operating system must have SOPHOS anti-virus installed
- The software is to be set to run **automatically** at noon each day by the main user of the machine (teacher or administrative officer). *See Appendix 2*

BACKING UP DATA

- The following data is to be backed up daily
 - SDrive/wp
 - SDrive/xl
 - SDrive/sims
 - Online diary
- The following data is to be backed up weekly
 - Macserver
 - Server2
- The following data is to be backed up monthly
 - Whiteboard Resources Folder
- Detailed instructions can be found in Appendix 3, 4 and 5

8 ISSUES TO CONSIDER FOR THE FUTURE

- The use of remote online storage facilities



Molescroft Primary School

Admin Data Backup and Anti- Virus Policy

Created on 11/9/2006 Reviewed September 2010

- Whether an unstable SIMS FMS package is the correct one to use for our financial management



Admin Data Backup and Anti- Virus Policy

Created on 11/9/2006 Reviewed September 2010

Appendix 1 Using AdAware SE Personal

Update the definition file

[Previous](#) [Next](#)

The definition file is Ad-Aware SE's detection list. It is based on Lavasoft's new Code Sequence Identification (CSI) technology and replaces the reference file used in earlier versions of Ad-Aware.

To make sure your computer is protected the definition file needs to be updated regularly. There are two ways to do this.

WebUpdate*

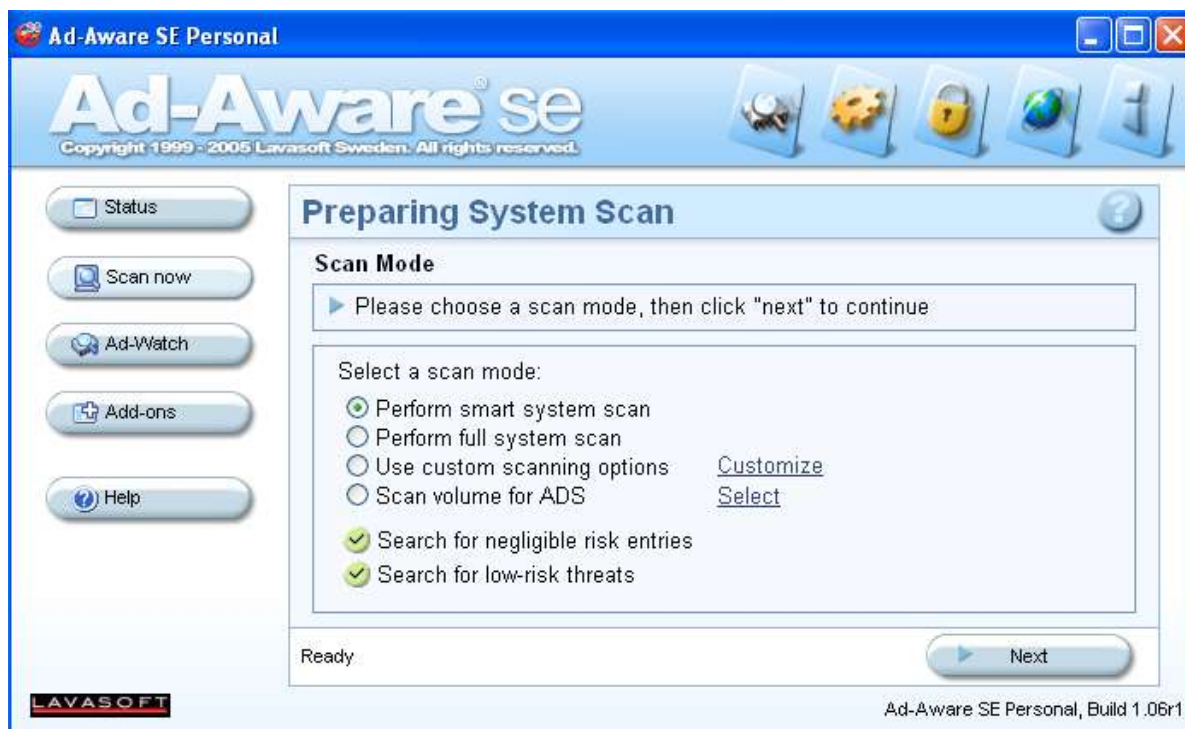
To start [WebUpdate](#) click the WebUpdate button in the toolbar or use the "[Check for updates now](#)" link on the [Status screen](#). Click "[Connect](#)" to check if a new definition file is available. If a new file is available click "[OK](#)" to download it. (The file will automatically be stored to the correct location on your computer.)

* You must be connected to the Internet to update the definition file

Preparing System Scan

[Previous](#) [Next](#)

Important Note! Before performing a scan, be sure that you have the most recent definitions file by using [WebUpdate](#). This can be done manually from the main status screen. See the [Getting Started](#) or [Update the definition file](#) chapters pages for instructions.





Admin Data Backup and Anti- Virus Policy

Created on 11/9/2006 Reviewed September 2010

Select scan mode

Perform smart system scan

The smart system scan is a fast system check and should be used only for daily system maintenance; i.e. you are sure that your system is clean and have performed a full system scan or an in-depth custom scan on your main hard drive at least once during the month. If this is your first scan, you suspect that your system has become infected with suspicious content, or you have used another antispyware product prior to installing and/or using Ad-Aware SE, please be sure to perform a full system scan (see below).

In most cases a Smart Scan will detect all content present on your system as Ad-Aware SE is capable of determining if further scanning is required. This does not include archived content however so a first time full system scan is highly recommended and at regular intervals to ensure that your system is clean.

When performing a smart scan the following scan settings are used:

- Full Memory Scan is performed
- Registry Scan is performed
- Deep Registry scan is performed
- Cookie-Scan is performed
- Favorites are scanned
- Hosts file is scanned
- Conditional scans are performed

Note! Smart scan does not scan within archives.

Perform full system scan

This is the in-depth scan mode that scans your whole computer for Spyware infections. The full system scan is highly recommended for the first time you use Ad-Aware SE, if you have reason to believe your computer is infected with Spyware which isn't found using the smart scan, or you have used another antispyware product prior to installing and/or using Ad-Aware SE. The full system scan is notably slower than the smart system scan, but has a higher probability of detecting Spyware infections in archives or that has been installed on drives other than your main hard disk.

The full system scan uses the same scan settings as the smart system scan, but also scans all fixed drives and archive files.

Use custom scanning options

You can customize Ad-Aware SE to scan on specific folders or drives. This option allows you to select or deselect drives and folders

Customize: Takes you to the Scan Settings screen. On this screen open the drive and folder selection screen by clicking on the "**Select drives & folders to scan**"

Scan ADS on drives/folders

The ADS (Alternate Data Streams) scan is performed in two steps. In the first phase, a regular disk scan is performed during which information is accumulated and cached. Any file scanned during this phase is being counted as a separately scanned object.

During the second phase detected streams are examined and, if appropriate, scanned. Every stream is counted as a separately scanned object during this phase. This design makes sure that the ADS scan does not bypass critical objects, just because they have none or are not attached to a DataStream.

Select: The ADS scan requires that the user manually selects one or more folders and/or drives to be scanned.



Admin Data Backup and Anti- Virus Policy

Created on 11/9/2006 Reviewed September 2010

Search for negligible risk entries

Negligible risk entries are not considered to be a threat. They consist of MRU (Most Recently Used items) lists which store information about the most recently used items, for example files, search words and programs. The MRU lists can be removed if the user desires.

Scan Summary

[Previous](#) [Next](#)

Shows a summary of the Scanning Results.

The screenshot displays the Ad-Aware SE Personal software interface. The window title is "Ad-Aware SE Personal". The main area is titled "Scanning Results" and contains three tabs: "Scan Summary", "Negligible Objects", and "Scan Log". The "Scan Summary" tab is active, showing a list of "Target families detected on this system" with one entry: "MRU List (36 Objects Total)". To the right of this list is a "Summary Of This Scan" box containing the following information: "Total scanning time: 00:02:12", "Objects scanned: 89977", "Objects identified: 0", "Objects ignored: 0", "New critical objects: 0", "Average TAC: 0.000", "Negligible objects: 36", and "Negligible references: 433". Below the list, there is a "Right-click an item for more options." prompt. At the bottom of the window, there are buttons for "Quarantine", "Show Logfile", and "Next". The status bar at the bottom left shows "0/36 Objects" and the bottom right shows "Ad-Aware SE Personal, Build 1.06r1".

Target families detected on this system: Sorts and lists the objects detected by target family. Clicking the [+] will show the TAC rating. Checking the box will mark all objects in the group for removal. This will be carried over into the Critical and Negligible Objects tabs as well; unchecking them will have the reverse action.

Summary of this scan: Shows the summary of the scan results in aggregate as well as display the total scan time. This information is also appended to the end of the log file.

Buttons

Quarantine: Puts the selected objects in a quarantine file. This can be useful when you don't want to quarantine all objects detected during a scan, as the automatic quarantine option does or to quarantine by family, vendor, or type of detected content. **Note!** You will be prompted to add a filename.

Show Logfile: Displays the log file created during the scan

Next: Takes you to the removal confirmation window



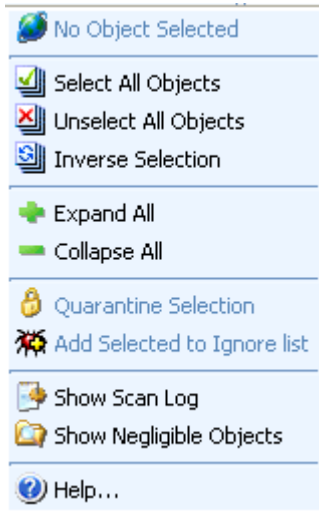
Admin Data Backup and Anti- Virus Policy

Created on 11/9/2006 Reviewed September 2010

Right-click to open the context menu where more options are available

Context menu

Show TAC page for "vendor name": Shows the TAC page for the target family*



Select all objects: Selects all objects found

Deselect all objects: Deselects all objects found

Inverse selection: Inverses the selection

Expand all: This will expand each family to show the TAC rating

Collapse All: This will collapse each family

Quarantine selected: Quarantines all selected objects. **Note!** You will be prompted to add a filename.

Move to ignore list: Adds the selected objects to the Ignore List

Show Critical Objects: Takes you to the Critical Objects tab

Show Scan Log: Takes you to the Scan Log tab

Show Negligible Objects: Takes you to the Negligible Objects tab

Help: Opens the Help file

* You must be connected to the Internet to access the TAC



Appendix 2

Using Sophos Anti-virus software

The ICT coordinator will setup the software on each PC.

He / She will also configure the software to do the following:

- To do an automatic full system scan everyday at noon
- Set the software to disinfect boot sectors and shred infected files.

Sophos updates itself daily.

If on scanning a virus is found the ICT coordinator must be told immediately, as removal of the virus often involves a long and complicated phone call to sophos.

Sophos Anti-virus does not protect your computer from viruses, it detects them.

NOTE : Both Sophos and Adaware must be in the the Startup Folder so that they start automatically when the computer is switched on.



Admin Data Backup and Anti- Virus Policy

Created on 11/9/2006 Reviewed September 2010

APPENDIX 3 BACKING UP WP/XL/SIMS

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 backup of the Calendar is also backed up to this folder.

Each morning the Admin Officers will move these files into the following folders (shortcuts for which are on the desktop):

- Monday Backup
- Tuesday Backup
- Wednesday Backup
- Thursday Backup
- Friday Backup
- End of Month Backup

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.

APPENDIX 3A BACKING UP WHITEBOARD RESOURCES FOLDER

At the end of each month the ICT Coordinator will back up the Whiteboard Resources folder to the Packard Bell 250 GB removable Hard Drive.



Molescroft Primary School

Admin Data Backup and Anti- Virus Policy

Created on 11/9/2006 Reviewed September 2010

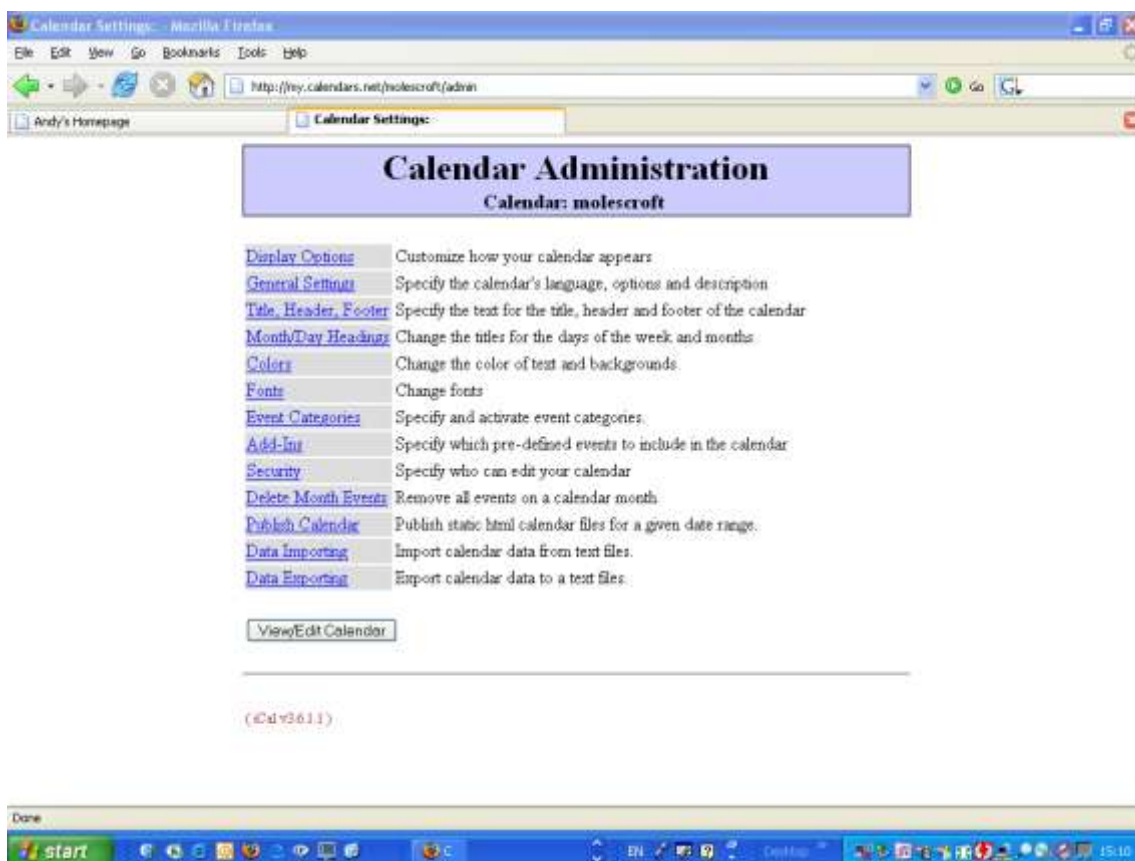
APPENDIX 4

BACKING UP THE ONLINE DIARY

The diary will be backed up daily by an Admin officer.

They will need to log on to the online diary and then click on administer this calendar.

This will bring up the following screen:





Molescroft Primary School Admin Data Backup and Anti- Virus Policy

Created on 11/9/2006 Reviewed September 2010

Select Data Exporting

Calendar Administration
Calendar: molescroft

Calendar Data Export
This allows you to export the calendar data to an ASCII text file. Simply specify the date range below and click Export.

Start Date End Date
Year Month Year Month
2007 February 2007 February

Output File Type: MS Outlook CSV Comma Separated Values (Windows)
 Tab Delimited
 CSV Comma Delimited

Comments:

All Periodic events are converted to Daily events before the data is exported.

MS Outlook CSV file is of a format that can be imported directly into Outlook.

The other two export options will produce a file with all iCal calendar attributes. These will include values for color, borders etc. The export file will have two record types: These are Single Daily events and Duration events.

Output Field Order Definition:

Single Daily Event Format
Seq, Date, Day, Event, Text, N, Repeat, Text, or HTML, X, Start Time, X, AM/PM, H, End Time, X, AM/PM, Y, Border, X, RecColor, H, ExColor, I

Select the dates that you wish to backup
Make sure that the TAB Delimited option is selected
Click on export



Admin Data Backup and Anti- Virus Policy

Created on 11/9/2006 Reviewed September 2010



Right click on molescroft.csv

Select save link as

Save work into mon backup folder on the desktop

The file is then copied into the same folders as wp/xl/sims backups

STEP 2

- From the Backup Calendar choose OPTIONS (at bottom of page)
- Choose Import Events
- Browse and find the file Molescroft.txt
- Choose to import the file as iCal (brown bear software)
- Choose import everything; don't check for duplicates
- Choose YES for delete all existing events before loading
- Click on Import Events
- When import has finished click on Done



Admin Data Backup and Anti- Virus Policy

Created on 11/9/2006 Reviewed September 2010

STEP 3

- Chose Export Events
- Choose Dates
- Field Separator = Comma
- Format = iCalendar
- Click on Download Events
- This will download an iCal file called CalciumEvents.
- Store this file with the other daily backups

What to do if the Diary backup needs to be restored.

In the unlikely event that both of the internet calendar providers disappear the following procedure needs to be followed.

- Open the Active Desktop Calendar on the Head teacher's laptop.
- Click on Data and then select Import Calendar
- Choose the most up to date version of the iCal backup (CalciumEvents)
- Click on open
- Import as a new layer
- Click on finish
- The calendar is now ready to be used

IPOD / ICAL USERS

The online calendar can be put onto your IPOD in the following way.

- Find the most up to date version of CalciumEvents in the backup folder
- In My Computer open ipod
- Open calendars
- Copy and paste CalciumEvents into calendars folder
- The Calendar is now ready to use

APPENDIX 5

BACKING UP THE MACSERVER

This backup is archived on to a tape. There are 2 tapes marked A and B. These are used on rotation. One tape should be kept by the ICT coordinator away from school.



Molescroft Primary School

Admin Data Backup and Anti- Virus Policy

Created on 11/9/2006 Reviewed September 2010

The backups are carried out automatically on Thursday evenings. The tapes should then be swapped on Friday morning.

The tape streamer is situated on top of the server in the old ICT suite.