SECTION 7 - VIRUS CONTROL

⇒ INTRODUCTION

This section is intended to give staff members a full understanding of viruses, their effects and preventative measures.

⇒ WHAT IS A COMPUTER VIRUS?

A computer virus is a program deliberately written to enter a computer without the user's prior knowledge. Viruses, although fairly simple to write, are usually created by programmers or people with a high level of computer literacy. The main aim of the virus is to cause general disruption although many cause actual destruction. Once the virus activates it will usually start destroying data, overwriting files or corrupting files.

⇒ HOW ARE VIRUSES CONTRACTED?

There are several ways in which a virus can be contracted, the undernoted are some of them:

- Downloading programs/files from the Internet.
- Downloading programs/files from Bulletin Boards.
- Receiving programs/files through email.
- Opening/Copying an infected file on your network drive.
- Opening/Copying an infected file from any write-able media (i.e. floppy disk, jazz drives, CDs, Tapes etc).

⇒ DIFFERENT TYPES OF VIRUS

Memory Resident
Loads into the memory upon running the infected file and stays there whilst the computer is switched on, where it can replicate easily. This effects .com / .exe / .pif / various data files.

Non-Resident
This type of virus can only infect other programs whilst the infected program is running.

Stealth
This type of virus will often reside on the hard disk of a computer completely undetected. It does this by re-directing virus checkers away from the infected files or hiding the itself.

Polymorphic
This is a virus which is written with code that repeatedly changes to disguise itself and appear as a different virus from the last detected.

Triggered Event
This is a virus that contains code, which will activate the virus on a certain date, keypress or command. For example, a virus may activate on the anniversary of a particular event.

In the Wild
This term refers a virus which has not been tested in laboratory conditions and has yet to be identified.

⇒ THE EFFECT ON HARDWARE

- Printing is not always possible.
- Communication port setting change.
- Dates and time change.
- System halts unexpectedly.
- Hard disk errors
- Mouse tracking changes.

Note: The above symptoms can be caused by problems other than virus presence and should always be reported to helpdesk.

⇒ THE EFFECT ON PERFORMANCE

Viruses will almost always cause a deficiency in performance, such as:

- The computer will take a long time to start up.
- Files take longer to open and save.
- System will appear to hang for several minutes.

Note: The above symptoms can be caused by problems other than virus presence and should always be reported to helpdesk.

⇒ VISIBLE EFFECTS / SYMPTOMS

Some viruses can remain on a system without any visible signs of infection, but some will display several features designed either to annoy the user or credit the author. These include:

- Messages appear at random on the screen.
- Text becomes wobbly, drips, disappears or hazes.
- Error messages appear.
- Pictures of famous people or events appear.
- The virus alerts you that you've been infected (usually in mocking terms)
- Music plays.
- Clicking noise comes from keyboard.
- Hard disk makes constant noise.

Note: The above symptoms can be caused by problems other than virus presence.

⇒ THE MACRO VIRUS

The Macro virus is the current biggest threat to library staff pc's. It is designed to run within a word processing package. The macro virus is very easily created and there are currently over 500 different macro viruses in existence and the number is increasing rapidly . Because of the speed of mutation in macro viruses, the virus scanner distributors are finding it increasing difficult to provide disinfectants. This is why it is extremely important to have up-to-date versions of your virus checker.

⇒ WM/CONCEPT VIRUS

Although the library network is scanned daily for viruses, we have had a problem with the WM/Concept Macro Virus, which infects Microsoft Word files. Once the user opens an infected Word document, the virus attaches itself to the Normal.dot file. The normal.dot file is the template file for all new documents in word and contains the default settings. As a result, after initial infection, it will continue to infect every new or opened document in word. This causes rapid infection and the user often doesn't know they have infected files until it is too late and they have distributed the infected file to others by saving it on the public network drives (drive K:). The symptoms are usually more annoying than harmful and include:

- Single key press results in many letters appearing
- Save as.....option on the file menu does not display drives.
- Particular words being typed will change (i.e. "the" will change to "and" etc).
- Sentences disappear after moving on to new paragraph.
- Messages appear along the bottom of the screen.
- Files becoming corrupt or deleted.
- Options disappearing from the menus.
- Error messages appearing (i.e. Basic Word Err7).

⇒ FINDING AND DISINFECTING VIRUSES

The Systems Department is constantly trying to combat the problem of virus infection and have employed a well-known virus detection kit which runs constantly in the background on the Common Desktop. The software is called MacAfee Virus check and is used throughout Edinburgh University. The way in which MacAfee functions means that Library staff members no longer need to remember to run regular virus checks on their personal files. The virus software delivers high speed scans of all files as they are accessed in real time, this protects the system far more efficiently than our previous software ever could. Detected viruses can be automatically cleaned, deleted, or even quarantined for future analysis and origin tracing.
E-mail and the internet represent the number one and fastest growing source of virus distribution. MacAfee's e-mail X-ray stops viruses hidden in e-mail attachments before they infect other users. Java and ActiveX scanning also prevent malicious Internet borne attacks.