

Anti-Virus Procedures

Author: Rachael Johnson

Version 1.0, January 2008

This Guide documents the procedures put in place by IT Services in order to implement the College's Anti-Virus Policy.¹

1. Anti-Virus Software

1.1 Desktop and Laptop Computers

Sophos Anti-Virus is provided under site licence agreement and is used to protect Microsoft and Apple-based systems throughout the College. IT Services (ITS) uses Sophos Enterprise Manager to update and manage the anti-virus software. Departments are required to use the centrally administered anti-virus software.

1.2 Servers

Sophos Anti-Virus is also used to protect the College Unix file servers from contamination, primarily by PC and Macintosh viruses which may infect files stored on Unix volumes. Departmental Microsoft Windows servers should also use Sophos Anti-Virus configured to allow automatic updates.

1.3 Mail Servers

College mail servers use a program called Amavis, which uses the Sophos program to check all incoming and outgoing *gold.ac.uk* email.

2. Email Attachments: Excluded File Types

ITS has a number of measures in place which are designed to minimise the risk of College systems becoming infected by email-borne viruses.

The table below lists the file types which are deemed unsafe for transmission by email from an external source to College email; internal email is also subject to the same exclusions. Any attachment which has one of the listed extensions or appears to be in a listed file format will be removed by College systems and the remainder of the message will be delivered as normal. Archive files ("zipped files") are checked for their constituent files: any comprising only files types which are considered safe will be allowed through; those containing any file types included on the banned list will be quarantined.

File extension	File type
.ani	Animated Cursor File Format
.bat	Batch processing file
.cab	Microsoft Cabinet Format
.cer	Microsoft Security Certificate
.chm	Compiled HTML Help File
.cmd	Batch File/Command File

¹ IT Services Guide V1.2 <www.goldsmiths.ac.uk/it/guides/v102.pdf>.

.cnf	Configuration File
.com	Command
.cpl	Windows Control Panel Extension
.cur	Cursor File Format
.exe	Executable File
.hlp	Windows Help File
.hta	Hypertext Application
.ico	Icon File Format
.ins	IIS Internet Communications Settings
.its	Internet Document Set, Internation Translation
.job	Microsoft Task Scheduler
.js	JavaScript Source Code
.jse	Jscript Encoded Script File
.lnk	Windows Shortcut File
.ma[dfgmqrstvw]	Microsoft Access Shortcuts and Stored Procedures
.mau	Media Attachment Unit
.md[az]	Microsoft Access Add Ins and Wizard Templates
.mhtml	Microsoft MHTML Document
.pif	Windows Program Information File
.prf	Windows System File
.pst	MS Exchange Address Book File
.reg	Registry Data File
.scf	Windows Explorer Command
.scr	Windows Screen Saver
.sct	Windows Script Component
.shb	Windows Shortcut Into a Document
.shs	Shell Scrap Object File
.tmp	Temporary File/Folder
.vb[es]	VBScript Files
.vsmacros	Visual Studio .NET Macro Project
.vs[stw]	Microsoft Visio Stencil, Template & Workspace Files
.wmf	Windows Meta File Format
.wsc	Windows Script Component
.ws[fh]	Windows Script Files
.xnk	Microsoft Exchange Shortcut

File types not included in the above table of exclusions are considered reasonably safe and can generally be transmitted by email.

3. Virus Outbreaks

Virus outbreaks on campus can become apparent via one or more sources, often simultaneously. An outbreak most frequently becomes apparent via ITS internal reporting mechanisms designed for this purpose, but may also originate from the Helpdesk or the Systems Administration team. Wider outbreaks may also be reported through external sources such as the JISC security mailing list, or via Sophos.

The procedure outlined below should be observed whenever new viruses, or variants thereof, are detected on campus, with the objective of containing their spread and preventing widespread disruption to IT services.

The designated IT Security Co-ordinator² will act as Virus Management Co-ordinator. There is also a designated Deputy IT Security Co-ordinator who can deputise when necessary.³

1) Outbreak notification can be triggered by:

- IT Security Co-ordinator
- The College JANET-CERT representatives⁴
- IT Services Helpdesk
- Systems and Networking team

2) The source triggering the outbreak alert sends a priority email to the *virus-alert@gold.ac.uk* email address. List membership comprises:

- ITS senior management team
- Help Desk
- Technicians

3) The source triggering the outbreak telephones the IT Security Co-ordinator on mobile phone (07866 497767) to initiate virus outbreak procedure if the likelihood is that the email has not been seen (annual leave, meetings, etc).

4) The Virus Management Co-ordinator takes the following action:

- Upon advice from JANET-CERT representative(s), requests that any necessary ports are blocked on the firewall, and appropriate network scans or log checks commensurate with a virus outbreak are carried out
- Provides Help Desk with an initial assessment and regular updates concerning the status and potential impact of the outbreak
- Administers the distribution of new .ide files where appropriate to all clients via Enterprise Console
- Manages the scanning of Unix file shares to detect, disinfect and/or remove infected files
- Co-ordinates any necessary technician visits to client machines, to include clean-up instructions
- In the case of College-wide outbreak, advises other departmental technicians of action to be taken⁵

² Currently Rachael Johnson.

³ Currently Suzanne Payne.

⁴ Currently Geoff Pryke and Steve Fuller.

⁵ A mailing list is to be developed for this purpose.

Considers the need to alert all staff via *gcinfo* in consultation with the Director of IT Services. Prepares mail to all staff, obtains authority to distribute. If email system is unavailable as a result of virus activity, emergency communication measures are to be used⁶

- Sends regular progress reports to *virus-alert@gold.ac.uk*.
- 5) Virus Management Co-ordinator terminates the alert by:
- Notifying *virus-alert@gold.ac.uk* when the alert is over and requesting the removal of any related messages
 - Requesting Systems and Networking team to remove blocks on network ports, if appropriate
 - Notifying relevant members of the user community that the alert is over.

⁶ Internal Communications is currently working on this.