PROTECTION OF INFORMATION SYSTEMS FROM COMPUTER VIRUSES, SPYWARE AND MALWARE

SUMMARY OF PRINCIPAL CHANGES

General changes	
This document has been subject to the annual review process led by the Chief Information Officer and has been re-issued with amendments, effective 1 September 2014.	
Section	
4.2	Refer to text

*(Amendments to version **03.0,** Appendix III, UPR IM01 are shown in italics.)*

Structure

1 INTRODUCTION

This document sets out the University's regulations and procedures for the protection of computer systems from computer viruses. It was originally approved by the Senior Executive Group with effect from 1 September 2001 *and has been amended with effect from 1 September 2014 on the authority of the Secretary and Registrar.*

2 DEFINITIONS

For the purposes of this document (Appendix III, UPR IM01) the following definitions apply. These definitions are additional to those given in section 2 of UPR IM01[1].

[1] UPR IM01 'Computer Networks, Security of Information Systems and the Protection of Information Systems from Computer Viruses'

2.1 **'computer virus, spyware and malware'**:

a self-replicating piece of software which may have the effect of disrupting an information system if introduced into it or a piece of software which, when introduced into an information system, extracts information to send to a third party or permits a third party to access that information system in some way;

2.2 **'approved detection software'**:

software that is used to detect and destroy computer viruses, spyware and malware, that has been approved for this purpose by the Chief Information Officer (or nominee);

2.3 **'principal user'**:

the person who normally operates the computer system;

2.4 **'portable media'**:

any portable media both from within and from outside the University.

3 SCOPE

These regulations and procedures apply to all persons accessing or using desktop services equipment which makes use of the University's computer networks (as defined in section 2.1, UPR IM01[1]). Such equipment would include computer workstations, laptops and other digital devices which are not owned by the University but, nonetheless, make use of its network and equipment loaned to staff for business use at home.

4 PROCEDURE

4.1 Heads of Strategic Business Units

Heads of Strategic Business Units will ensure that local computer systems security policies incorporate appropriate monitoring procedures to ensure compliance with all of the regulations set out in this document and will designate a member of staff within their area (a 'designated person') who will be responsible to them for ensuring compliance with these regulations.

4.2 Virus detection software

4.2.1 *The Chief Information Officer is responsible for the distribution, installation and updating of the approved virus detection software on University systems, services and computing equipment across the University.*

4.2.2 *Where appropriate, the Chief Information Officer will arrange for the approved virus detection software to be available to designated authorised persons who will then be responsible for distributing and/or installing the software and any subsequent updates to it, on all computer systems for which they are responsible.*

4.2.3 *All approved virus detection software that is in use within the University, by its wholly-owned subsidiary companies or their wholly-owned subsidiaries, must be updated at least daily.*

4.2.4 *It is the responsibility of the designated staff as authorised by the Chief Informations Officer to install the latest version of the approved virus detection software on all of the computer workstations that it commissions or re-commissions.*

5 GENERAL REGULATIONS

5.1 Security updates

5.1.1 All desktop services equipment and mobile devices must be kept up-to-date with any operating system security updates which may be issued by the operating system manufacturer.

5.1.2 It is the responsibility of each user to ensure that updates are installed as soon as they become available. Where possible, systems should be configured to automatically check for the availability of updates and to download and install them. Otherwise a manual check for new updates should be performed at least once a week.

5.1.3 All new desktop services equipment and mobile devices or those which have be re-commissioned should be installed without a network connection until detection software has been installed and the equipment is ready to have security updates applied.

5.2 Computer viruses, spyware and malware

5.2.1 All desktop services equipment and mobile devices must be capable of running the approved detection software. The Head of Procurement and Budget Holders will ensure compliance with this regulation.

5.2.2 All desktop services equipment and mobile devices must have up-to-date approved detection software installed and active at all times.

5.2.3 It is the responsibility of each user to ensure that:

a the approved detection software successfully downloads and applies any updates that may be available;
b a full scan is undertaken not less than once each month;
c all portable media and any files that they may have downloaded, including files attached to email messages, are scanned before they are opened;
d all files and/or disks sent to others, either within the University or externally, are free of viruses, spyware and malware before they are sent.

5.3 Members of the University using personal privately-owned devices to connect to and make use of the University's network must also comply with the provisions of 5.1 and 5.2 above.

6 PROCEDURES FOR REPORTING THE PRESENCE OF A VIRUS, SPYWARE AND MALWARE

6.1 The detection of a virus, spyware and/or malware must be reported to the Helpdesk immediately. As much as possible of the following information should be made available to the Helpdesk:

a the name or type of virus, spyware or malware;
b how the virus, spyware or malware was detected;
c the extent of the infection (whether a single computer workstation or a group of computer workstations or a server is affected);
d the source of the virus, spyware or malware;
e whether there may be other recipients of the infected file;
f the steps that have been taken to eliminate the virus, spyware or malware.

6.2 Users should refrain from broadcasting warnings regarding real or apparent viruses, spyware or malware and from passing on such warnings received from others.

7 GUIDANCE

The Chief Information Officer will ensure that appropriate guidance and support is provided on the staff intranet and by the Helpdesk to enable all users to meet the responsibilities placed on them by the regulations and procedures set out in this document.

Mrs S C Grant
Secretary and Registrar
Signed: **1 September 2014**