Anti-Malware and Endpoint Protection Policy

Version	Date	Changes	Author	Approved by
0.1 Draft	February 2019	New Policy	Chris Linton	
1.0	February 2019	No changes	Chris Linton	Seamus Doyle
1.1	June 2022	Removed Symantec reference added exceptions	James Vincent (Cyber Security Manager)	Ian Purdy
1.2	January 2026	Title and policy amended to include “Endpoint protection”	James Vincent (Cyber Security Manager)	James Vincent

Introduction

This Policy sets out the responsibilities of all users that connect to the University IT facilities, in relation to malicious software.

The word ‘malware’ is used collectively to denote many types of malicious software, including but not limited to, viruses, ransomware, worms, Trojans, macros, mail bombs and rootkits.

A malware infection is potentially costly to the University and could result in the loss of data or access to IT systems. Malicious software can spread from an infected system and can lead to severe disruption to IT services and possible reputational damage or even fines.

Scope

This Policy applies to all users, including users of privately owned devices that connect to the University IT facilities. By following this Policy, users will help to protect themselves and other University users against malicious software.

Purpose

The objectives of this document are:

- To set out user responsibilities about malicious software prevention
- To set out the rules governing the application and use of malicious software prevention systems at the University

Policy

- All University owned personal computers and servers that are connected to the University network or otherwise using the IT facilities must run the University approved and up-to-date anti-malware product or endpoint protection that continually monitors for malicious software.
- Computers and tablets supported by Digital & Information Services will have the University approved anti-malware product or endpoint protection pre-installed.
- The University provides a copy of the approved anti-malware or endpoint protection product for Windows®, Linux® and Apple® Desktops.
- Users who do not choose the approved anti-malware or endpoint protection product for their privately owned devices, must have anti-malware protection that meets the requirements described here.
- Anti-malware or endpoint protection must be configured for on-access scanning, including the downloading or opening of files, folders on removable or remote storage, and web page scanning.
- Anti-malware or endpoint protection protection software must be configured to run regular scans.
- Do not try to uninstall or disable anti-virus software or endpoint protection. Any messages suggesting that antivirus or endpoint protection has been disabled should be reported immediately.
- If users experience difficulties with the approved anti-malware or endpoint protection product, requests for technical support may be made through the IT Service Desk on (028) 9097 3760 or by email itservicedesk@qub.ac.uk or online at https://it.qub.ac.uk/sitehelpdesk/user/log.asp
- The University reserves the right to disconnect any device from the network if an infection is found or suspected. The device will be disconnected until the infection is removed and suitable preventative tools have been installed on the device.
- If you suspect that a device is infected with a virus, report the incident immediately to the IT Service Desk on (028) 9097 3760 or by email itservicedesk@qub.ac.uk or online https://it.qub.ac.uk/sitehelpdesk/user/log.asp and / or to your school IT staff.
- Email attachments must be scanned by an anti-virus product before delivery.
- Individuals may be subject to disciplinary action if this Policy is breached.

Exceptions

All exceptions must be approved by the Cyber Program Board and recorded in this document.

- High Performance Computing (HPC) systems
- Any other devices as approved by the Cyber security manager