THE ROSE LEARNING TRUST

ANTI-MALWARE POLICY

Date	**September 2019**
Prepared by	**Information Security Consultant**
Review Date	**September 2020**
Version	**V1**

1 PURPOSE

This is an internal policy that defines how The Rose Learning Trust protects its information assets from malware.

2 RESPONSIBILITIES

All users, inclusive of employees, subcontractors and suppliers with direct access to The Rose Learning Trust information technology systems are expected to conform to this policy.

The Rose Learning Trust's IT service provider are responsible for providing support to users in complying with this policy.

The Rose Learning Trust's Chief Projects Officer is responsible for ensuring that this policy is annually reviewed and that changes are made in the event of legislation change or compliance frameworks such as the Cyber Essentials scheme are updated

3 SOFTWARE APPROVAL

The Rose Learning Trust prohibits any form of software that hasn't been approved and formally documented on The Rose Learning Trust's Approved Software Register in the SecureSchools cyber security management software

4 ANTI-MALWARE SOFTWARE

All information technology assets of The Rose Learning Trust must have the organisation's designated anti-malware software installed where such software is compatible. All new assets must be commissioned using the Workstation Secure Configuration Checklist

4.1 Designated Anti-Malware Software

The Rose Learning Trust has chosen Sophos Intercept X as its designated anti-malware software solution

4.2 Anti-Malware Software Configuration

The Rose Learning Trust's anti-malware software will be configured to perform:

- On-access scanning of files and web pages
- On-access scanning of removable media
- Scheduled full system scans daily
- Daily definition database updates

4.3 Anti-Malware Review

The Rose Learning Trust will perform an internal audit on a sample of 5 workstations every 6 months to ensure that the anti-malware software is performing the tasks defined in 4.2

5 USER AWARENESS TRAINING

All employees and contracted staff at The Rose Learning Trust are mandated to remain conversant with recognising and defending against malware threats. The Rose Learning Trust provides the platform for employees to refresh their knowledge through the SecureSchools cyber security management solution.

All employees and contracted staff are encouraged to opt-in to the SecureSchools Cyber Threat Briefing, which provides timely advice and recognition techniques for current malware threat

6 ATTACK SIMULATION AND PERFORMANCE MONITORING

The Rose Learning Trust will perform a simulated malware attack using the SecureSchools cyber security management software every 6 months to test the effectiveness of its technical controls and awareness levels of its staff.