PATCH MANAGEMENT POLICY

Date	**September 2020**
Prepared by	**Information Security Consultant**
Review Date	**September 2021**
Version	**V2**

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

1 PURPOSE

The Rose Learning Trust has a responsibility for ensuring the security requirements of its information assets are met. As defined in its information security policy, these requirements include confidentiality, integrity and availability. Malware that exploits software vulnerabilities presents the risk of breaching security requirements. Processes defined in this policy will reduce the risk of software vulnerabilities being exploited by malware threats. This internal policy applies to all *physical* and *software* assets listed in The Rose Learning Trust's information asset register

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 WORKSTATIONS

The Rose Learning Trust ensures that all its workstations are running an operating system that is actively supported by the vendor according to its development life cycle. Workstations running retired or legacy operating systems are removed from service. Automatic updates are enabled for all workstations' operating system, updating at the default frequency defined by the vendor

4 PATCHING SCHEDULE

The Rose Learning Trust aims to install all security patches within 30 days of release and aims to install patches not related to security within 90 days

5 PROBLEMATIC PATCHES

The Rose Learning Trust's IT service provider will take all reasonable measures to ensure that updates known to be problematic are prevented from being installed until resolved by the vendor.

6 SOFTWARE LICENCING

The Rose Learning Trust does not operate unlicensed software and takes all reasonable measures to ensure that it meets all End User Licence Agreement terms

7 LEGACY SOFTWARE

The Rose Learning Trust takes all reasonable measures to ensure that the software it uses is supported by its vendor. There may be occasions where no alternative software is available; in this case the software must be approved by the Operations Manager and marked as unsupported in the organisation's information asset register

8 MONITROING AND INTERNAL AUDIT

The Rose Learning Trust conducts annual internal vulnerability scans and 6-monthly external vulnerability scans on its network boundary and websites using the SecureSchools cyber security management software to ensure compliance with this policy.