Patch Management Policy

1. Purpose

Chelmsford County High School for Girls (CCHS) 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 CCHS's information asset register.

2. Responsibilities

All employees with direct access to the CCHS information technology systems are expected to conform to this policy.

CCHS's IT Team are responsible for providing support in complying with this policy.

The IT Manager 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

CCHS 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. Workstations patches are monitored by Microsoft Endpoint Configuration Manager.

4. Servers

CCHS ensures that all its servers are running an operating system that is actively supported by the vendor according to its development life cycle. Updates are installed manually during quiet periods to ensure the minimum of disruption to service during normal working hours, in line with the patching schedule. Server patches are monitored by WSUS.

5. Other Hardware

All other hardware (e.g., Switches and Firewalls) will be updated manually during quiet periods to ensure the minimum of disruption to service during normal working hours, in line with the patching schedule. Hardware going out of vendor support or no longer supported by the vendor will be added to the asset replacement plan.

6. Patching Schedule

CCHS aims to install all security patches within 14 days of release and aims to install patches not related to security within 90 days.

7. Problematic Patches

CCHS's IT Team will take all reasonable measures to ensure that updates known to be problematic are prevented from being installed until resolved by the vendor.

8. Software Licensing

CCHS does not operate unlicensed software and takes all reasonable measures to ensure that it meets all End User Licence Agreement terms. Any unlicensed software located on any device will be removed as soon as possible.

9. Software Patching

CCHS ensures that all licensed software is kept up to date and updated within 90 days of release.

10. Legacy Software

CCHS 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 IT Manager and marked as unsupported in the CCHS information asset register.

11. Monitoring and Internal Audit

CCHS conducts annual vulnerability scans to ensure compliance with this policy.

Change Log

Version	Changes	Author	Change Date	Approval Date
0.1 – Draft 1.0 - Approved	First draft based on Secure Schools Ltd model policy.	Tony Cable	12th May 2022	22nd June 2022

Approved by	Facilities & Finance Committee
Date Approved	22nd June 2022
Date of Next Review	June 2023
Model Policy	Secure Schools Ltd