Secure Schools

Information Security Policy

Patch Management Policy

1. Purpose

Aspire Federation 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 Aspire Federation's information asset register.

2. Responsibilities

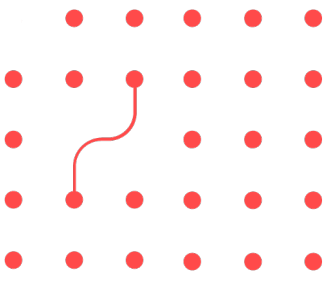
All employees with direct access to the Aspire Federation information technology systems are expected to conform to this policy.

Aspire Federation's Zulogic/ Cantium are responsible for providing support in complying with this policy.

Emma Hickling 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

Aspire Federation 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

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

5. Problematic Patches

Aspire Federation's Zulogic/ Cantium 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 Licensing

Aspire Federation does not operate unlicensed software and takes all reasonable measures to ensure that it meets all End User Licence Agreement terms.

7. Legacy Software

Aspire Federation 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 Emma Hickling and marked as unsupported in the Aspire Federation information asset register.

8. Monitoring and Internal Audit

Aspire Federation conducts annual vulnerability scans to ensure compliance with this policy.

Approved by	
Date Approved	
Date of Next Review	