Patch management is the process of managing and applying software updates and fixes to computer systems, software applications, and network devices to address security vulnerabilities, improve performance, and enhance security.

Effective patch management is critical for maintaining the security and integrity of IT systems and networks to reduce the risk of security breaches, data loss, and downtime by known vulnerabilities.

**Patching Processes**

With reference to the DfE Cyber Security Standards for Schools and Colleges, all online devices and software must be licensed for use and should be patched with the latest security updates.

You must avoid or replace unpatched or unsupported hardware or software, including operating systems. These devices are the most popular targets for successful cyber attacks.

Ask your IT Service Provider to make sure that all devices and software are set up to meet technical requirements in the DfE Cyber Standards. Subscribing to services rather than buying items can be a way to help achieve this. This is known as Software as a Service (SaaS).

Remember that patches often require downtime as systems may need to reboot to successfully apply the updates, so it might be prudent to ask school to staff to fully power down their devices at least once a week to ensure that essential security updates can be applied.

**Reasons for Patch Management**

Patching is essential for several reasons:

|  |  |
| --- | --- |
| **Security** | Patching software helps address known vulnerabilities and security flaws that could be exploited by cyber attackers to compromise systems. |
| **Data Protection** | Patching helps to protect sensitive information from unauthorised access, theft, or loss, and ensures compliance. |
| **System Stability** | Patches often include bug fixes that improve performance. |
| **Risk Management** | Patching is a fundamental aspect of risk management and mitigates security risks associated with vulnerabilities in software and systems. |
| **Maintaining Trust** | Patching demonstrates a commitment to security and protecting personal data which enhances trust among users and stakeholders. |
| **Cyber Resilience** | Patching is a key component of cybersecurity aimed at building your cyber resilience. By applying patches as soon as possible, you can better defend against evolving cyber threats and enable faster recovery from cyber incidents or threats. |

**How to protect yourself**

Hackers rely on you to ignore those ‘annoying’ update notifications so they can get in before the update is made – so don't give them the chance. Updates may be applied automatically; but sometimes you may be prompted to install the update, which you should do.

Your school should be working towards meeting the [DfE Cyber Security Standards for Schools and Colleges.](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges)

**Assessment of importance**

With reference to the DfE Cyber Standards, your school must have automatic updates enabled.

You must complete manual updates to hardware or software, including configuration changes, within 14 days of the release of the patch where the vulnerability is:

* described as high risk or worse
* has a Common Vulnerability Scoring System (CVSSv3) score of 7 or above

The Common Vulnerability Scoring System is the security industry standard for measuring the danger of a vulnerability. The score is a number from 1 to 10 where 10 is the most dangerous. There is a more detailed explanation of CVSSv3 on the NVD website.

When notified by the Department for Education (DfE), patches should be applied within 3 days of notification. This will only be done in instances of dangerous zero-day attacks where institutions are at immediate risk and there is a suitable patch available.

**Make Patching Easier**

By implementing strategies, schools can streamline the patching process and improve the security posture of the school.

* Ensure automatic updates are enabled across your devices and systems
* Have scheduled time when users completely shut down devices to enable any updates to install, or to allow IT Support Teams to perform maintenance to minimise disruption
* Have an up-to-date device inventory which details operating system versions
* Remove unsupported devices and unnecessary software from the network
* Sometimes users may be prompted to install an update which they should do at the earliest convenient opportunity
* Educate users on the importance of patching and cybersecurity
* Regular monitoring of devices to identify those missing critical updates

Effective patch management is crucial for protecting sensitive data and ensuring the reliability and security of the school IT infrastructure.

You can refer to NCSC Guidance on patching:

[Install the latest software and app updates - NCSC.GOV.UK](https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates)

[The problems with patching - NCSC.GOV.UK](https://www.ncsc.gov.uk/blog-post/the-problems-with-patching)