Title	**BWT Security Update Management Policy**
Associated Policies	• Acceptable Use Policy (TPO/GU/06) • Data Protection (TPO/STA/25) • Freedom of Information (TPO/QA/03) • Online Safety (TPO/STA/12) • Electronic Communications – Use and Management • Mobile working policy

REVIEWED: March 2025 **NEXT REVIEW: March 2027**

1. Policy Statement

1.1 In order to ensure that the Trust's information assets are kept secure at all times, it is necessary to identify and manage technical vulnerabilities and patching.

1.2 The purpose of this policy is to set out the ways to ensure that the Trust IT assets are not vulnerable to known security issues for which fixes are available by identifying technical vulnerabilities and managing the implementation of patches for third party operating systems and software.

1.3 Security update management refers to the maintenance of Trust owned and provided IT systems in order to keep them up to date and secure. Security updates are released to mitigate identified vulnerabilities. Updates can include but are not limited to:

- Updates released on a regular cadence, such as monthly
- Updates which are automatically applied when released by the vendor
- One-off updates to bring software up to a version that the vendor will continue to support
- Specific security patches, which are sometimes categorised as 'Out of Band' patches

1.4 This policy is not currently intended to cover operating system version, application feature upgrades or quality patches that improve or enhance the usage of a product.

2. Who does this policy apply to?

2.1 This policy applies to all Brooke Weston Trust's users, systems and equipment.

2.2 All devices that process, store, or transmit the Trust's confidential, staff, student or personal information have audit and logging enabled, where logging is possible and practical.

3. Who is responsible for carrying out this policy?

3.1 The implementation of this policy will be the responsibility of RM as the Trust's IT Managed Service Partner (MSP) and other suppliers as appropriate. It will be monitored by the Senior Leadership Team and will remain under regular review by Brooke Weston Trust and its suppliers.

4. Technical Vulnerabilities

4.1 A vulnerability is commonly defined as "an inherent weakness in an information system, security procedures, internal controls, or implementation that could be exploited by a threat source."

4.2 These vulnerabilities are constantly being found and corrected via software updates or patches. Unfortunately, it is not always the developer or user who discovers these vulnerabilities. When discovered by a potential attacker the vulnerability becomes something to be exploited for gain and kept secret for as long as possible. A newly discovered vulnerability is often referred to as a "zero-day exploit" and is difficult to defend against.

4.3 The Trust's managed service partners will ensure that they maintain awareness of the technology components for which they are responsible along with information from vendors and other sources to identify security vulnerabilities as they become available. This should include:

- Operating systems e.g. Windows, Linux, Cisco
- Databases e.g. SQL Server
- Web servers e.g. IIS, Apache
- Desktop software e.g. Office, Acrobat
- Web technologies e.g. browsers, Java
- Application software e.g. SIMS
- Hardware e.g. servers, routers

4.4 Each managed service partner must put in place a process to ensure that all relevant information about updates is being received and reviewed by competent staff members. This will usually give guidance about the Trust's specific level of risk and urgency associated with each update.

4.5 Where configuration changes are recommended to close off vulnerabilities, these must be actioned through the Trust's and RM's change management process so that appropriate controls are in place for testing, risks assessment and backout.

4.6 For hosted and cloud services, the responsibilities of the cloud service provider (CSP), RM and the Trust must be defined and agreed. This may involve the CSP being responsible for vulnerability assessment and patching for some or all aspects of the service, depending on the cloud service model adopted (e.g. IaaS, PaaS or SaaS or similar service definitions).

4.7 In addition to the ongoing review of system vulnerabilities and vendor-supplied software updates, the Trust conduct a vulnerability assessment at least annually. The breath and focus of the vulnerability assessment will be guided by consideration of the level of risk associated with IT systems.

5. Security Update Management

5.1 Patches and updates will typically be issued by software vendors on a regular schedule as cumulative packages. These will be linked to the specific version of software that they relate to and may have dependencies stipulated with other software modules, products or operating systems.

5.2 Procedures will be put in place to obtain copies of the software updates electronically when they are issued by the vendor. The scheduling of the installation of updates will depend upon several factors including:

- The criticality of the systems being updated
- The expected time taken to install the updates (and requirements for service outages)
- The degree of risk associated with any vulnerabilities that are closed by the updates
- Co-ordination of the updating of related components of the infrastructure
- Dependencies between updates

5.3 The Trust will endeavour to deploy patches for significant vulnerabilities within 14 calendar days of an update being released. Significant means vulnerabilities classified as:

- Critical or High Risk
- A Common Vulnerability Scoring System (CVSS) v3 score of 7 or above
- No classification or level of vulnerability issued by the vendor

5.4 The Trust will endeavour to deploy patches for vulnerabilities not classified as significant within 30 calendar days

5.5 Where necessary an update release plan may be created and maintained to keep track of when various systems will be updated, considering the factors listed above. The plan must be managed through the change management process. For updates that are low risk and regular, a standard change may be defined within the change management process to allow this to happen without excess administrative overhead.

5.6 Where appropriate, patching of software, particularly of security updates, will be automated and the success of the process regularly checked and reported to the Trust.

5.7 Updates will be carried out during planned maintenance windows where possible, so as to minimise disruption to systems availability. However, the Trust reserves the right to carry out security updates at any time, which may result in individual systems or the entire network being unavailable for a period of time

6. Unsupported software

6.1 The Trust will endeavour to ensure that all software and systems remain maintained and supported and where appropriate utilise the latest version of software through the implementation of this policy. If unsupported components are identified that are required to support the Trust's or a school's critical operational activities, then a risk assessment will be carried out to ascertain and agree the correct approach to rectifying the issue. Options may include upgrading to a newer version, user of an alternative product or through device isolation/firewalling. Unsupported components that present undue levels of risk may be removed from the network, devices and / or systems.

6.2 Trust's asset register will hold information such as the reference to the vendor's support statement and the date at which updates will no longer be provided. The asset register will be used to inform decisions about component removal and will be kept up to date in alignment with decisions made and actions taken.

7. Responsibilities

7.1 The following table identifies the party responsible for ensuring security updates are applied to the identified system or component:

System / Component	Party responsible for vulnerability management and patching
Microsoft Windows Servers	RM
Managed Microsoft End User Devices	RM
Network Switches	RM
Antivirus	RM
Firewalls	Network provider
Server hosted applications	RM
Cloud business applications	Application provider

7.2 Trust-nominated systems administrators are responsible for ensuring the system(s) they manage are kept up to date in alignment with this policy

7.3 All users of Trust IT systems are responsible for supporting the Trust's security update processes:

- A user must not interfere with or prevent the update of a system
- If requested to do so, a user must carry out action to support the update process, e.g. log out of a system, reboot a device or connect a device to the Trust network
- If a user identifies that an update mechanism is not working, they must report it

8. Monitoring and Review

8.1 This policy will be monitored as part of the Trust and Academy's annual internal review and reviewed on an annual basis or as required by legislature changes or following IT system changes which may impact vulnerability and update management.

Document Control

Date of last review:	March 2025	**Author:**	MRO
Date of next review:	March 2027	**Version:**	1.0
Approved by:	SDG	**Status:**	Non-statutory

Summary of Main Changes: v 1.0

- Initial document incorporating RM's draft update policy