Title	**System Logging and Monitoring Policy**
Associated Policies	• Acceptable Use Policy (TPO/GU/06) • Safeguarding and Child Protection (TPO/HS/05) • Professional and Safe Conduct (TPO/STA/10) • Data Protection (TPO/STA/25) • Freedom of Information (TPO/QA/03) • Online Safety (TPO/STA/12) • Electronic Communications – Use and Management

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 monitor the use and activities of both authorised and unauthorised users across the Trust's systems to identify any actions that are not in keeping with the acceptable and secure use of the facilities provided.

1.2 The purpose of this policy is to set out the ways in which such operational and security event monitoring of users and systems must be carried out for purposes such as:

- Ensuring effective Trust, academy and IT operations including:
  - resolving a technical issue
  - checking for viruses or other network threats
  - updating and maintaining devices/software belonging to the school
  - checking compliance of devices/software belonging to the school
  - obtaining information related to academy business.

- Investigating and responding to potential security incidents:
  - Unauthorised access attempts
  - Unusual use of privileged accounts e.g. administrator
  - Attachment of unauthorised removable media devices
  - Unusual patterns of activity e.g. late at night
  - Changes to system settings

- Investigating unauthorised use where there is a breach with academy policies, procedures or standards
- Prevention or detection of crime
- Compliance with a Subject Access Request, Freedom of Information Request or any other legal obligation.

1.3 Event logs should be produced, regularly reviewed, and kept in line with log retention needs considering the legal and regulatory requirements, industry best practice, and the specific needs of the Trust.

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. Event Logging

4.1 All clients, servers, cloud resources and other equipment (such as network routers and switches) involved in hosting the storage or processing of the Trust's data and information will have the available audit logging facilities activated to allow the recording and monitoring of activities in at least the following areas:

- Dates and times of key events e.g. log on/log off
- Successful and rejected systems access attempts
- Successful and rejected data and other resource access attempts
- Changes to system parameters and configurations
- Use of system utilities and applications

5. Event Logging Access Control

5.1 Access to logs will be controlled through permissions, and to ensure that the content of log files being cannot be altered or tampered with after they have been written.

- Event logging and monitoring is performed by authorised personnel only.
- Where possible, system administrators should not have permission to erase or de-activate logs of their own activities.
- Where personally identifiable information (PII) is recorded as part of logging activities, appropriate access control must be in place to prevent such data being used for any other purpose.

5.2 Storage capacity of the log file media should be adequate to prevent limits being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

6. Clock Synchronisation

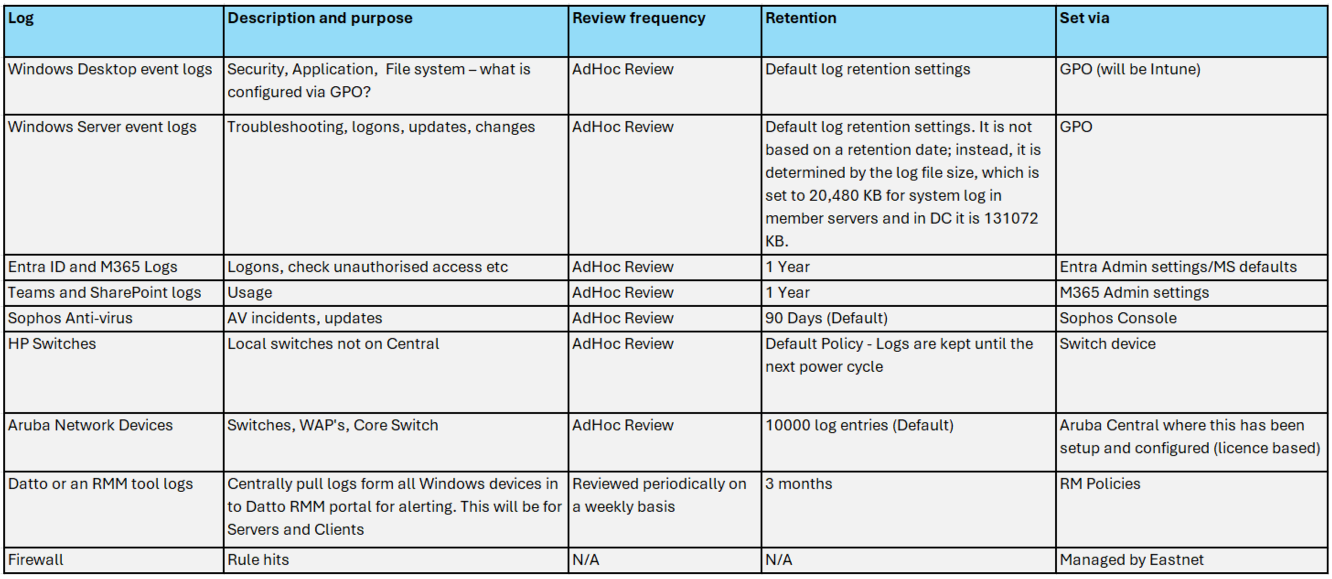
6.1 The clocks of all relevant information processing systems within an organization or security domain should be synchronised to a single reference time source.

7. Event Log Monitoring and Log Retention

7.1 Systems and logs are monitored and retained for a period as shown below. The contents of audit logs will be reviewed according to the:

- Business criticality of the systems
- Classification of the information assets involved
- Frequency with which systems have been attacked or compromised previously
- Level of exposure to external networks

7.2 High risk events should automatically alert to RM's incident management process where possible.



Log	Description and purpose	Review frequency	Retention	Set via
Windows Desktop event logs	Security, Application, File system – what is configured via GPO?	AdHoc Review	Default log retention settings	GPO (will be Intune)
Windows Server event logs	Troubleshooting, logons, updates, changes	AdHoc Review	Default log retention settings. It is not based on a retention date; instead, it is determined by the log file size, which is set to 20,480 KB for system log in member servers and in DC it is 131072 KB.	GPO
Entra ID and M365 Logs	Logons, check unauthorised access etc	AdHoc Review	1 Year	Entra Admin settings/MS defaults
Teams and SharePoint logs	Usage	AdHoc Review	1 Year	M365 Admin settings
Sophos Anti-virus	AV incidents, updates	AdHoc Review	90 Days (Default)	Sophos Console
HP Switches	Local switches not on Central	AdHoc Review	Default Policy - Logs are kept until the next power cycle	Switch device
Aruba Network Devices	Switches, WAP's, Core Switch	AdHoc Review	10000 log entries (Default)	Aruba Central where this has been setup and configured (licence based)
Datto or an RMM tool logs	Centrally pull logs form all Windows devices in to Datto RMM portal for alerting. This will be for Servers and Clients	Reviewed periodically on a weekly basis	3 months	RM Policies
Firewall	Rule hits	N/A	N/A	Managed by Eastnet

8. Monitoring and Review

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 logging and monitoring.

Document Control

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

Summary of Main Changes: v1

- Initial document reflecting main policy, RM log reviews and current log retention settings