FIREWALL POLICY

Date	**September 2020**
Prepared by	**Information Security Consultant**
Review Date	**September 2021**
Version	**V2**

Date	**September 2019**
Prepared by	**Information Security Consultant**
Review Date	**September 2020**
Version	**V1**

1 PURPOSE

This is an internal policy that defines how The Rose Learning Trust installs, configures and maintains firewalls at the boundaries of its IT infrastructure.

2 RESPONSIBILITIES

All users, inclusive of employees, subcontractors and suppliers with direct access to The Rose Learning Trust information technology systems are expected to conform to this policy.

The Rose Learning Trust's IT service provider are responsible for providing support to users in complying with this policy.

The Rose Learning Trust's Chief Projects Officer 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 BOUNDARY FIREWALLS

The Rose Learning Trust installs a firewall at every boundary between the internal Local Area Networks and the Internet. The Rose Learning Trust Boundary Firewalls are physical appliances and are an enterprise model from either Cisco, Watchguard, Sonicwall or Sophos

The Rose Learning Trust requires boundary firewalls to have the following capabilities supported and enabled:

- HTTP and HTTPS proxy
- Gateway antivirus
- Intrusion Prevention System
- Advanced Persistent Threat protection

4 PERSONAL FIREWALLS

The Rose Learning Trust ensures that the Personal Firewall is enabled on all network connected endpoints that have such ability. Personal firewalls are configured with a default deny policy, never a default allow policy

5 FIREWALL ADMINISTRATION

All Boundary Firewalls are administered only from the Local Area Network. All remote connections to the administrative interface on boundary firewalls are blocked from the outside world

All Personal Firewalls are administrable through centralised management; Microsoft Group Policy, Windows Intune, or the 3rd party security vendor if included in a host-based security solution

6 BLOCKED SERVICES

The Rose Learning Trust does not allow services that are identified by the NCSC, GCHQ or the Cyber Essentials scheme as 'vulnerable' to be allowed to connect through firewalls. Services that are identified as vulnerable are as follows:

- SMB
- TELNET
- NetBIOS
- tFTP
- RPC
- rLogin
- RSH
- rExec

Denial of these services is tested annually as part of the Cyber Essentials certification.

7 RULE APPROVAL

The Rose Learning Trust maintains a register of all approved firewall rules permitted on boundary firewalls using the SecureSchools cyber security management software. Rules are approved only by the Chief Projects Officer with support from the SecureSchools team.

Where an endpoint with a Personal Firewall has a non-generic configuration, a manual Firewall Rule Register will be uploaded to the SecureSchools software.

8 INTERNET ACCESS

Access to the internet from The Rose Learning Trust's Local Area Networks is granted only to devices that require access as an operational necessity. Restriction of access is implemented by a default deny policy.

9 MONITORING AND INTERNAL AUDIT

The Rose Learning Trust conducts vulnerability management and 6-monthly external vulnerability scans on its boundary firewalls using the SecureSchools cyber security management software to ensure compliance with this policy