Our Lady of Good Help

Catholic Primary School

Firewall & Filtering Policy

Chair of Governors	Mrs S. Devereux
Headteacher	Mr M. McQuiston
Date adopted: September 2023	**Review Date:** September 2024

'Like Our Lady, we live wisely, think deeply and love generously in Christ.'

Index

1. Process Introduction

Our Lady of Good Help contracts MGL, as leading educational IT experts, to manage our firewall and filtering procedure and policy. This procedure establishes a framework for understanding the policy and risks relating to internet filtration and firewall facilities using Smoothwall. This procedure establishes a framework for initial setup of the filter/firewall, and changes to the filter/firewall once in use to mitigate risk by providing a process for changes to the system. This backup policy links to the IT Security Policy for the overall management of onsite systems (MGL held policy).

1.1 Scope

This process covers the firewall and filtering provided by Smoothwall which is the on premise solution to manage the delivery of the Internet Service Provision. The process ensures data and web access is managed to standards expected by DfE and NCSC for appropriate filtering and appropriate monitoring of internet services in school.

1.2 Process Owner

Andrew Procter, the Services Director for MGL is responsible for defining/refining this Process.

1.3 Process Responsibility

The MGL Technician, the School Computing Lead and the Headteacher.

1.4 Process [Quality] Control

The Services Director reports to the Managing Director, who is responsible for detecting and correcting any problems with the processes. There is direct consultation between the Services Director and Managing Director in the event of any S.L.A. not being met.

1.5 Process Approval

The Firewall and Filtering Policy is part of the technical services contract provided by MGL. Annual management meetings take place at which firewall and Filtering service provision is discussed and agreed to ensure it is compliant with the schools IT security Policy and Safeguarding Policy. In the event that there is no formal objection, at regular intervals the services are deemed to be accepted for the preceding period. Product Descriptions for services and/or contracts give details of the scope of the internet service provision contracted by the school.

2.1 Policy Introduction

This document describes the standard firewall and filtering policy that should be adopted for schools using Smoothwall as part of MGLs ISP service. This policy must be implemented to ensure safe and secure use of the internet for pupils, staff and guests at the schools. Any issues that arise should be raised with the MGL help desk immediately.

Effective filtering security depends not only on technical measures, but also on efficient policies,

procedures and continual 'good user' education and training. The school is responsible for ensuring that the infrastructure and network is as safe and secure as is reasonably possible by utilising the measures outlined below:

- Users can only access data which they have a right to access.
- Access to personal data is securely controlled in line with the School's General Data Protection Policy.
- Logs of access are maintained by Users whilst they are using the system.
- Effective guidance and training for Users is in place.
- There are regular reviews and audits of the safety and security of the computer systems.
- There is overview from senior leaders who have an impact on policy and practice.

2.2 Scope

This policy applies to all technology systems, including but not limited to, computers, laptops, servers, mobile devices used by the education establishment. Personal devices if connected to the school network will also be in scope.

2.3 Firewall and Filtering operation

The school is responsible for ensuring that the procedures approved within this policy are correctly implemented and that the relevant school personnel will receive guidance and training to effectively carry out their responsibilities.

MGL is responsible for ensuring that the procedures approved within this policy are correctly implemented and that the relevant MGL personnel will receive guidance and training to effectively carry out their responsibilities.

MGL will manage and maintain the Smoothwall firewall and filtering system to ensure:

- The Firewall and Filtering system will be set up according to standard Smoothwall education core policies to ensure that it meets the recommended technical requirements for NCSC appropriate filtering and monitoring.
- The Firewall and Filtering system will be managed to ensure that it meets the recommended technical requirements for NCSC appropriate filtering and appropriate monitoring.
- Devices are protected by Https inspection and require a Https interception certificate for secure filtering.
- Updates to the filtering system take place on a termly basis or sooner if there is an urgent manufacturer release.
- Responsibilities for the management of filtering security are assigned to appropriate and well-trained staff.
- The firewall will be managed by MGL. Any changes requested to the firewall must be logged via the MGL helpdesk with technical justification. All changes will be logged in the helpdesk for future reference.
- The filter will be managed by MGL. Any changes requested to the filter must be logged via the MGL helpdesk with technical justification. All changes will be logged in the helpdesk for future reference.

The school will ensure the following activities takes place:

- Request any changes to the firewall or filtering system by logging a request on the MGL helpdesk facility. All requests must be agreed with the School DSL.
- Termly reviews and audits of the safety and security of filtering systems will take place using the testfiltering.com website by SWGfL.
- Access to filtering system changes will be limited to MGL technical support personnel.
- Responsibilities for the management of filtering security are assigned to appropriate and well-trained staff.
- All users will have clearly defined internet access rights whilst using the School filtering systems; details of access rights available to groups of users are managed by MGL and will be reviewed annually or on the request of the school.
- An appropriate system is in place for Users to report any actual / potential filtering incidents to MGL who will review the issue.
- 'Acceptable Use' policies and agreements are in place for Staff, Students and Community Users who are permitted on any school devices that are subject to filtering.
- Users must not attempt to use any programmes or software that may allow them to bypass the filtering / security systems in place to prevent access to such materials.

2.4 Training and Awareness

Members of staff will be made aware of the school's Acceptable Use Policy for using the Internet. Staff will be provided with training on data protection and internet security.

Pupils will be made aware of the school's Acceptable Use Policy for using the Internet. Staff will monitor and raise any issues that may arise when observing lessons.

2.5 Filtering Policy Statement

The Filtering of internet content provides an important means of preventing users from accessing material that is illegal or inappropriate in an educational context. The filtering system however cannot provide a 100% guarantee as web content changes dynamically on a regular basis. It is therefore important to acknowledge that filtering only forms one element in a larger strategy for online safety and acceptable use.

Internet access is filtered for all users; differentiated internet access is available for staff and customised filtering changes are managed by MGL. Illegal content is filtered by the filtering provider by actively employing the Internet Watch Foundation, Google Safe search and other illegal content lists such as Open DNS. Google SafeSearch is enforced to all users via a content modification in Smoothwall.

Filter content lists are regularly updated by Smoothwall automatically; and internet use is logged and monitored by the Smoothwall reporting system.

Where personal mobile devices are permitted access to the school's network, filtering will be applied that is consistent with other onsite devices. This does not apply if mobile phones are using 4G/5G connections, as they do not go via the schools filtration system.

Enhanced / differentiated user-level or group level filtering is provided through customised the use of the Smoothwall filtering programme by MGL Technical staff. By default the system is set up to differentiate

between Pupils and Teachers for differing policy levels.

Should technical staff have to switch off the filtering system for any reason or for any User, this must be logged and carried out by a process agreed with the Headteacher.

Requests from Staff for sites to be removed from the filtered list will be considered by the School DSL who will consult the Headteacher. Any agreed requests will be recorded by logging a ticket on the MGL Helpdesk requesting allow or block.

Any issues with the filtering system will be reported immediately to the MGL Helpdesk.

Staff will be made aware of the filtering systems through the Acceptable Use Policy, training on induction and regular briefings at staff meetings and inset days.

Parents will be informed of the school's filtering policy through the Acceptable Use policy and online safety awareness sessions and newsletters.

Any change in the control of filtering or any filtering incidents will be made available to:

- The computing lead, Headteacher and DSL
- Governor Wellbeing committee
- MGL
- Local Authority / Police upon request

The filtering security will be reviewed in response to the evidence provided by the audit logs of the suitability of the current provision, testing of the filter by the school, or advice from DfE, NCSC or Smoothwall.

2.6 Firewall Policy Statement

The Firewall facility provides a firewall to block unwanted external access to the internal school network and systems.

The firewall will be set up in a standard Smoothwall recommended configuration.

Firewall passwords will be unique for the school firewall system and be amended from the manufacturer supplied password. The password will be complex. MGL will store passwords for reference if required.

The firewall cannot be customised by the school. All requests for customisation must be logged as a ticket on the MGL Helpdesk with technical justification. All customisations should be minimal in terms of port forwards required. By default all ports except 443 will be blocked for inbound access.

The Police Cyber Alarm should be set up by the school to ensure there is a facility for early warning attacks on the firewall.

2.7 Monitoring

The monitoring process will alert the School to breaches via the Safeguarding reports; an internal school procedure needs to be in place for managing safeguard reports and any identified breaches to the filtering system.

Daily safeguard reports will be sent to the school DSL for review.

An instant alert will be configured to send an instant alert for danger category safeguard issues to the DSL

via email.

Testing of the filtering system will take place termly by the School DSL lead to check appropriate filtering is working on test devices using testfiltering.com.

2.8 Policy Review

This policy will be reviewed annually by the MGL Technician and School management to ensure it remains relevant and effective in protecting the education establishment's technology systems and sensitive information.

2.9 Acceptable Use

All employees, students, and contractors must comply with the education establishment's acceptable use policy when using technology systems.

Penalties for non-compliance: Failure to comply with the Firewall and Filtering policy may result in disciplinary action, including termination of employment or termination of access to technology systems.

2.10 Approval

This Firewall and Filtering policy has been approved by the education establishment's management and is effective immediately.