Bonner Primary School

Firewall Policy

Confidence, respect and a love of learning

Our vision and aims support Articles 3, 28, 29, 30 and 31 of the United Nations Convention on the Rights of a Pupil.

Article 3: The best interests of a child must be a top priority in all things that affect pupils.

Article 28: Every child has the right to an education.

Article 29: Education must develop every child's personality, talents and abilities to the full. It must encourage the child's respect for human rights, as well as respect for their parents, their own and other cultures, and the environment.

Article 30: Every child has the right to learn and use the language, customs and religion of their family.

Article 31: Every child has the right to relax, play and take part in a wide range of cultural and artistic activities.

Approved by:	Governors Committee	**Date:** February 2020
Last reviewed on:	February 2020 – Next Review February 2022	
Next review due by:	Spring Term 2022	

Introduction and Scope

London Grid for Learning in conjunction with Bonner Primary School manage a perimeter firewall between its' Internet connection with LGFL between Bethnal Green and Bonner Mile End to establish a secure environment for the school network and computer resources. This firewall filters Internet traffic to mitigate the risks and potential losses associated with security threats to the school network and information systems.

In addition the firewall secures a number of other 'zones' controlling traffic between servers and other parts of the data network.

The perimeter firewall is a key component of the Network Security Management.

Purpose

The purpose of this policy is to define standards for provisioning security device. These standards are designed to minimise the potential exposure to
the loss of sensitive confidential data, intellectual property, safeguarding, damage to public image etc., which may follow from unauthorised use of school resources.

This policy establishes procedures for the schools perimeter firewall administration, determines the technology standard used by the firewall hardware and software, assigns firewall administration responsibilities and defines the filters applied to our school network.

Responsibilities

The IT Technicians liaise with London Grid for Learning to ensure perimeter activities are closely monitored.

While responsibility for information systems security on a day to-
day basis is everyone's responsibility specific guidance and direction for information systems security is the responsibility of the Co-ordinator and IT Technicians.

Policy for Perimeter Firewalls

The perimeter firewall permits the following outbound and inbound Internet traffic:
• Outbound - LGFL generates a weekly report which is uploaded to the support site for authorised school staff to access.

• Inbound - Allow Internet traffic that supports the mission of the school and is in accordance with defined system, application and service policies.

Reason for filtering ports or applications:

• Protecting Internet Users - LGFL
• Protecting our outbound bandwidth - LGFL
• Protecting the rest of the Internet - LGFL

Firewall Standards

LGFL is committed to operating fully supported and maintained resilient firewalls.

Access to read or write firewall configurations for both internal or perimeter devices are required to be by unique identity which can be logged.

Operational Procedures (Perimeter security)

Bonner Staff may request that access be granted from the Internet to services inside Bonner School/LGFL for a new or existing application or service. These requests must be approved, authorised and submitted to the ICT Co-ordinator.

The Co-ordinator or LGFL will evaluate the risk of opening the firewall to accommodate requests. Where the risk is acceptable, granting of requests will be dependent on network infrastructure limitations and the availability of required resources to implement the request. If the risk associated with a given request is deemed objectionable, then an explanation of the associated risks will be provided to the requestor and alternative solutions will be explored.

Periodic Review of Firewall Settings

Reviewed weekly.