

11 October 2012

LGfL 2.0 Option 2

**NOT RECOMMENDED by LGfL for
the Majority of Schools**

Ian Lehmann

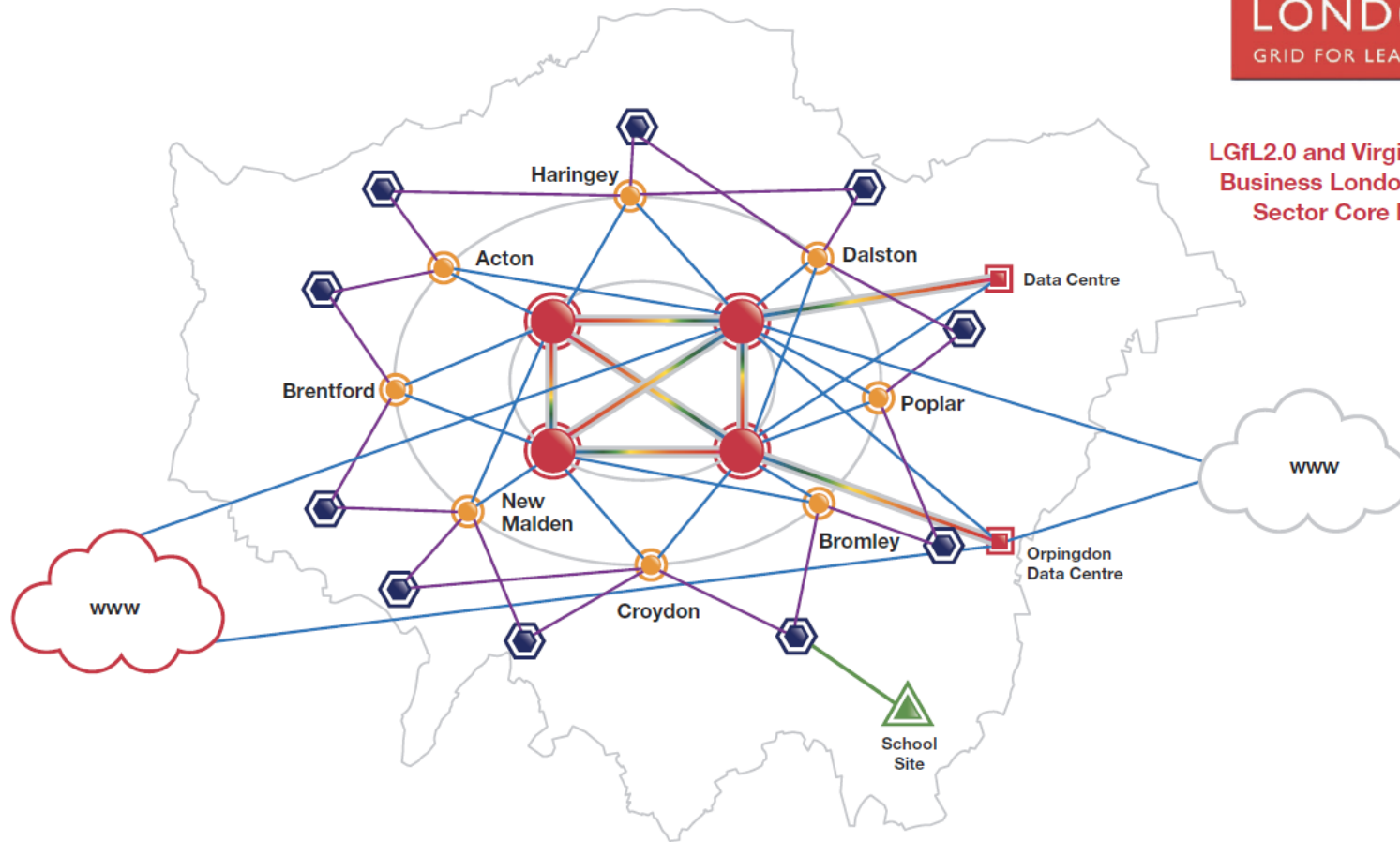
Chief Operations Officer

London Grid for Learning

LGfL 2.0 Network

LONDON
GRID FOR LEARNING

**LGfL2.0 and Virgin Media
Business London Public
Sector Core Network**



 Inner Core
Provider Devices

 Core Provider
Edge Devices

 Aggregation Point
(54 pan London)

 Inner Core & Outer Core

 4 X 10Gb

 n x 10Gb

 n x 1Gb

 10Mbps – 1000Mbps
connections to schools

Powered by



Standard LGfL 2.0 firewall offers...

Default Networks:

- Admin
- Curriculum

Optional Networks:

- VC (Video Conferencing)
- VoIP (IP telephony)
- WLAN (Wireless)

LGfL Security Guidance

Information, guidance and safeguards regarding Remote Access products

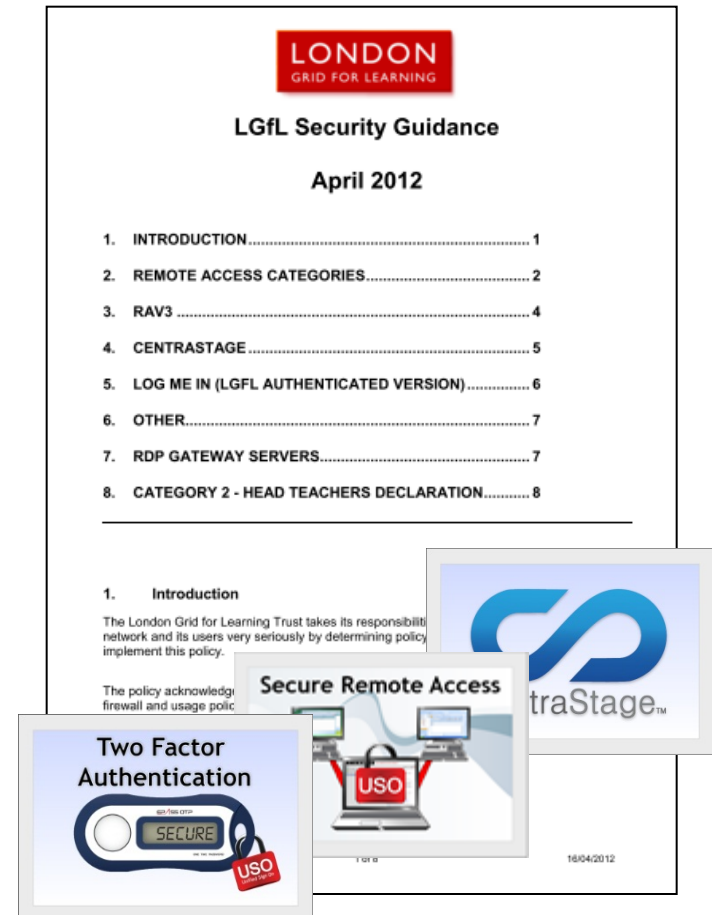
LGfL categories of web-based Remote Access products

Head Teacher authorisation

Two-factor authentication (USO-OTP)

LGfL USO-authenticated LogMeIn

RDP gateway service



Option 2

OPTION 2 – Public IP addresses with school's own managed firewall

This option is suitable for a school which wishes to have total control over, and responsibility for, network security. LGfL will supply the school with a number of public IP addresses to use on its own firewall. The quantity of IP addresses supplied will depend on current and expected usage. All firewall policies and options such as Network Address Translation (NAT) are administered by the school.

Option 2

- School has an LGfL-supplied CPE and firewall as usual, plus an additional 'raw' Internet port enabled on the CPE, to which it can connect its own firewall/network.
- MIPs and firewall rules are NOT supported on the standard LGfL-managed firewalls for Option 2 schools.
- Access to most LGfL 2.0 services is still possible:
 - Per-user URL filtering via the LGfL-managed firewall (this connection uses the school's LGfL-assigned 10. IP range)
 - VMB Network Statistic Portal instead of LGfL support site. (1 day course)
 - Email relay & outgoing MailProtect available subject to conformity with SMTP security - see next slide.

Option 2 Mail Server

If a school adopts Option 2 and has its own local mail server operating on a public IP address then, subject to appropriate configuration of the school's firewall, it can receive email from the Internet (if the domain's MX records are correctly configured), and also post email directly out to the Internet.

If the school wishes to use LGfL MailProtect to scan incoming messages, then it is necessary to change the domain's MX records to point at MailProtect. The MailProtect system will then deliver messages on to the school's local mail server via its public IP address.

Outbound use of LGfL MailProtect is possible, subject to the secure configuration of SMTP ports.

So, alongside the necessary firewall rules, DNS for the school's domain(s) controls how mail is delivered *into* the school, while the configuration of the school's local mail server controls how mail is delivered *out* to the Internet.

Option 2 DNS

For those schools not wishing to run their own DNS servers, upstream DNS servers are provided for Option 2 schools by Virgin Media Business.

194.168.4.123

buscache1.service.virginmedia.net

194.168.8.123

buscache2.service.virginmedia.net

Option 2 Web Filtering

Schools can choose to take complete control over web filtering by running their own in-house filtering system and routing all web traffic via the CPE's Option 2 port.

For schools wishing to use the LGfL 2.0 WebScreen™ 2.0 filtering system, this can be arranged either by using the LGfL 2.0-assigned 10. IP ranges internally and routing all web traffic via the LGfL-managed firewall, or by setting up a local proxy server that performs one-to-one NAT between the school's local network and the LGfL-managed firewall. Per-user filtering using USO accounts is possible in both of these situations.

It is the school's responsibility to configure and deploy web filtering correctly. External consultancy regarding the setup of this service is available at an hourly rate.

LGfL Option 1 services

Video Conferencing, VoIP & WLAN services are available via the LGfL-managed firewall.

DNS hosting is available by arrangement with the Service Desk, along with web site hosting using the Plesk environment, and Sophos anti-virus software.

Premium content is available as normal.

LGfL 2.0 Option 2 Advantages

- School can configure firewall rules including MIPs at any time, in any way.
- Closest thing to 'raw' Internet access.
- May be an easier transition for existing LGfL1 Option 2 schools.

LGfL 2.0 Option 2 Disadvantages

- The school must buy its own firewall, and fund in-house or external staff to manage this firewall and all other aspects of network security.
- A wrongly-configured firewall could expose the school's local network to attack from the Internet and/or other Option 2 LGfL schools on any port.
- Attack bandwidth from another school will be the smaller bandwidth of the two schools.
- Attack bandwidth from the Internet will be the bandwidth of the school.
- **This option is NOT RECOMMENDED by LGfL for the majority of schools.**

Steps to become Option 2

- First, the Head Teacher or Principal of the school must approve the declaration entitled 'LGfL 2.0 Option 2' on this page of the support site: <https://support.lgfl.org.uk/secure/myacc/ht/declarations.aspx>
- Next, contact Mark Tremain at LGfL, on (020) 8274 3416, to request a RIPE NCC IP address form that must be filled out and returned.
- An SCR can then be raised with Virgin Media Business, after which the public IP range will be configured on the school's CPE.
- Once the school advises the Service Desk that they are ready to switch to Option 2, a 72 hour grace period will start, after which all previously-configured MIPs and firewall rules will be removed.