

*Please keep this important document in a safe place for future reference*

# LONDON Grid for Learning

**Making the most of your LGfL**

*Safeguarding - a guide to LGfL security*



<b>Safeguarding : A Guide to LGfL Security .....</b>	<b>2</b>
Introduction .....	2
Nominated Contacts .....	2
The Head Teacher .....	3
Designated Data Manager (Head Teacher Proxy).....	3
Two-Factor Authentication .....	4
<b>Security Services .....</b>	<b>4</b>
WebScreen - Internet filtering .....	4
Remote Access utilities .....	4
Sophos anti-virus protection.....	5
“Option 2” – Raw Internet .....	5
MailProtect - Email filtering .....	6
Guidance on access to the Head Teacher Portal within the Support Site .....	6
<b>Related Questions.....</b>	<b>7</b>
What if I believe the connection is slow? .....	7
What if our connection is not working?.....	8
If my MIS is not supported by LGfL’s data extraction process – why not?.....	9
Can LA or Council personnel still support schools on LGfL 2.0? .....	9
Don’t you know who I am? .....	9
In summary .....	10
<b>What else comes with LGfL 2.0 as well as broadband? .....</b>	<b>10</b>
<b>E-Safety guidance</b> .....	11
Internet filtering .....	11
Industry strength email.....	11
Email scanning.....	11
Unified Sign On.....	11
USO FX- Secure File Transfer .....	11
AutoUpdate.....	11
Office Apps and Skydrive – shareable online storage .....	11
Antivirus protection .....	11
Website hosting .....	12
Video central HD .....	12
Podcasting.....	12
Secure Remote Access .....	12
CentraStage.....	12
OpenCheck .....	12
Unified Helpdesk .....	12
Network Management and Security .....	12
Training .....	12
<b>What else is available from LGfL? .....</b>	<b>13</b>
Gridstore .....	13
Internet Telephony.....	13
Wi-Fi .....	13

This booklet provides a guide to LGfL security services. Additional guidance and substantial resources relating to the safeguarding of pupils and staff is available online at [www.SAFETY.lgfl.net](http://www.SAFETY.lgfl.net)

For information on all the included LGfL Curriculum Content and Resources please visit [www.CONTENT.lgfl.net](http://www.CONTENT.lgfl.net)

# Safeguarding : A Guide to LGfL Security

## Introduction

In many contexts there is an interplay, a trade-off, between freedom and security. Imagine a road system with no rules or conventions – in one sense, absolute freedom but also a complete absence of safety. Some people become irritated by the delays caused by security measures before boarding a plane but we all understand and appreciate why these inconvenient restrictions are imposed upon us.

Like the real world, the online world has become more complex and more threatening. The Internet is an open system, it is almost a perfect anarchy, and as a consequence it is simultaneously wonderful and dangerous. Just as security and regulation has increased over time in travel systems such as air and road, the London Grid for Learning has needed to evolve the balance between security and facility in providing safe educational broadband connectivity to schools, in a changing environment.

One of the primary reasons schools choose to use LGfL is because of the comprehensive measures taken to keep children safe when going online.

The purpose of this paper is to ensure school leaders are fully informed of and appreciate the security measures which LGfL has in place (notably since the opportunity afforded by the rollout of the new LGfL 2.0 network) and also to be aware of how to tailor these to the particular circumstances of individual schools.

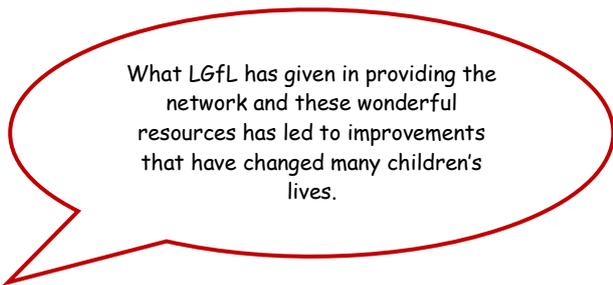
## Nominated Contacts

To formally represent the school in the administration of LGfL services each school must have at least one, ideally several, persons who have been formally approved by the Head Teacher (HT) as an LGfL Nominated Contact (NC).

NCs have a key role in the interface between LGfL and service users within the school, and their responsibilities include managing user access (i.e. usernames and passwords) and adjusting the settings of systems such as Internet filtering.

The names of existing NCs for a particular school and how to create new ones can be found at [www.USO.lgfl.net](http://www.USO.lgfl.net)

NCs have access to the LGfL 2.0 Helpdesk (020 8255 5555) and have the ability to raise cases online via the LGfL Support Site ([www.SUPPORT.lgfl.net](http://www.SUPPORT.lgfl.net)). Some HTs will decide to appoint themselves as NCs for their schools. This is a perfectly good idea for those comfortable with the role, but must be done proactively, as NC status is not automatically applied to HT accounts.



It is strongly recommended that all NCs attend **training** in order to become familiar and confident with the matters for which they have responsibility, and to support the NC and the school in maximising the benefits which can be derived from LGfL services. LGfL 2.0 Training is free (Ts & Cs apply) and details can be found via [www.TRAINING.lgfl.net](http://www.TRAINING.lgfl.net).

### **The Head Teacher (or Head of Centre/Service/Establishment)**

Within the context of Data Protection legislation, it is generally understood that it is the Head Teacher or Principal, with authority delegated by the governing body, who acts for the school in its role as "Data Controller". For this reason it is the Head Teacher, or a formally-appointed delegate, who must engage with LGfL at certain key points in relation to LGfL and its supply partners acting as "Data Processors", and also in the management of network components which affect access to personal data and other assets.

Approvals or authorisations given by the Head Teacher/Delegate are typically undertaken online through the LGfL support site, and for this purpose an individual LGfL USO\* username and password is required. ( \*USO = Unified Sign On – for each staff member and pupil, one username and password to remember which gives access to all the LGfL systems, services and content, which are appropriate to the individual.)

Head Teachers play an undeniably vital role in the deployment of sensitive services in a school environment. It is therefore crucial that LGfL support personnel can actually identify and verify the identity of a Head Teacher *in post*. Heads can assist LGfL in this process by ensuring that school websites, stationery, EduBase entries, and LA or council websites display consistent and up-to-date public-facing information about their appointment. This will reduce delays otherwise introduced by conflicting published information concerning the identity of the Head Teacher.

### **Designated Data Manager (Head Teacher Proxy)**

If required, a Head Teacher may formally nominate a 'proxy', who can act as the Designated Data Manager (DDM) on behalf of the school in respect to the matters covered in this document, and on related matters which may arise from time to time that would otherwise require authorisation from an 'in post' Head Teacher. This person should be a trusted and prudent DBS checked senior professional who has sufficient insight and understanding of the related issues to make sound judgements on behalf of the school and is contracted to do so. This user would be empowered to interact with LGfL/Atomwide in all matters as would the HT themselves, with the exception of being unable to appoint a second person to the role of 'Proxy' on behalf of the actual HT.

The appointment of a **Designated Data Manager** (or 'Head Teacher Proxy') requires an 'in post' Head Teacher to complete and sign a delegation form, and for this to be uploaded as a support case via the LGfL support site requesting the appointment. The form is available from the 'Downloads' section of the USO Support Site, found under the 'Resources' tab.

Acknowledgement of the role is limited to activities within the USO Support Site (and related micro-sites, such as those for VoIP and MailProtect), and any other mode of contact with LGfL/Atomwide Service Desk staff. The relevance of holding NC status and whether or not to possess a registered OTP tag (see next section), applies equally to DDMs and HT account holders.

## Two-Factor Authentication

To underpin security, and in addition to a password, some actions require a second level of security which is achieved by means of a small personal device known as an 'OTP tag' which provides a 'one-time' digital password, for each login. It is strongly recommended, (and in some circumstances it is a requirement), that the Head Teacher and each NC registers an OTP tag. For information on ordering OTP tags, please refer to [www.OTP.lgfl.net](http://www.OTP.lgfl.net).

## Security Services

### WebScreen - Internet filtering

Your school's LGfL subscription includes a sophisticated Internet filtering service which can be tailored to a school's particular preferences and is capable of supporting multiple policies - for example, a more open policy for staff than for pupils. [www.WEBSCREEN.lgfl.net](http://www.WEBSCREEN.lgfl.net)



The initial filtering settings applied to a new LGfL 2.0 connection are, by intention, relatively strict; this is so that a school can relax certain required areas as appropriate, rather than starting with 'doors wide open' and no awareness of how to close them.

Any NC can apply to be assigned responsibility for administering the school's filtering policies by raising a support case on the support site. As indicated previously, it is strongly recommended that NCs attend training in the use of the WebScreen 2 filtering system.

The World Wide Web is a dynamic system which grows with the addition of millions of new pages every day. To filter such a huge resource, the WebScreen system utilises **artificial intelligence** to scan and evaluate pages which have not previously been visited and categorised. This can result in a short delay while the system completes the necessary interrogations and assessments. The delay is regrettable, but the alternative is either 'give the page without scanning', or block the page. It is not possible to pre-categorise every page in advance (although millions of pages are) as the World Wide Web is too vast and grows too rapidly for any system to achieve this.

### Remote Access utilities

Remote Access is a technology which enables persons located outside your school to access or take control of computers and other devices connected to your school's network. In order to safeguard pupils, teachers, personal data and valuable IT systems, the LGfL applies a rigorous approach to the management of Remote Access.

As an integral part of its service, LGfL provides a secure and preferred means of Remote Access by licensing for all connected schools a service known as **RAv3** which is based on industry-standard Cisco technology. Together with USO authentication, RAV3 provides a regulated and audited means for authorised Remote Access by staff. Though perhaps initially unfamiliar with RAV3, staff users adopting this technology have quickly become confident and able to accomplish tasks successfully.

**LogMeIn Rescue**, a widely-used Remote Access product, is available in an enterprise version from LogMeIn which is authenticated by USO and is also, like RAV3, CentraStage and RDP Gateway, approved as a "**Category 1**" Remote Access product for use with LGfL. LogMeIn subscriptions are not provided by LGfL, and the integration has principally been facilitated in order to allow access to supported products and devices in schools by external support companies and organisations (although a small number of in-house school IT support teams do also make use of it).

Certain other products are approved as "**Category 2**" utilities. Use of these products requires adjustments to the school's LGfL firewall, which in turn reduces the degree of protection that this device provides and hence requires authorisation by the Head Teacher (or Designated Data Manager). This authorisation is implemented through the Head Teacher portal section of the support site and requires that the school's Head and all NCs have OTP tags.

It is not possible to specify or quantify the exact risk to which a school is exposed as a consequence of authorising Category 2 products, but the change might be likened to opening a window, which equally allows a breeze or a thief to enter.

For further information on Remote Access, and other services available to assist schools including CentraStage, and LGfL's RDP Gateway service, please review the LGfL Security Guidance available at [www.POLICIES.lgfl.net](http://www.POLICIES.lgfl.net).

### **Sophos anti-virus protection**

LGfL saves schools a significant cost by including within the LGfL package virus protection for every computer and server within the school, including all teachers' laptops. Even at home, or away in the long summer break, staff laptops can be kept protected against the latest virus outbreaks, using a personal USO account to authenticate access to the update system from anywhere online.

Through the purchase of these licences in enormous bulk, the cost per device is a tiny fraction of what an individual school would pay, and hence is included within your school's LGfL subscription.

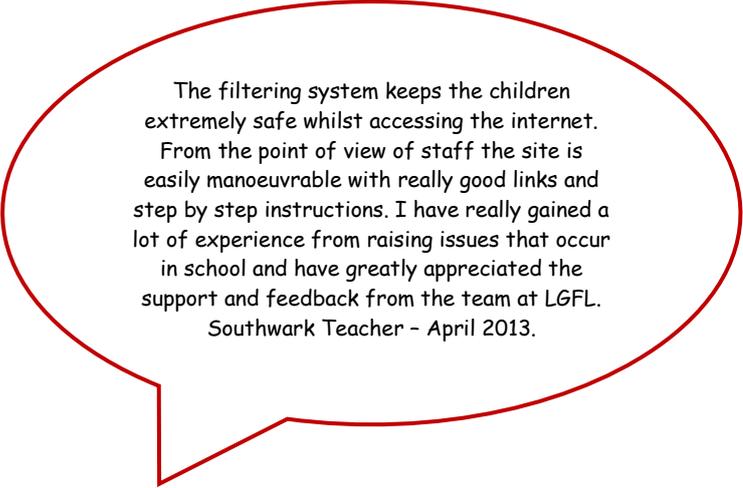
Viruses infect computers and networks, and among other things affect the operation of legitimate software, use your computer to infect and interfere with your contacts' computers, and consume storage space and network capacity. In extreme cases, a virus outbreak could shut down your school network and do irreparable damage. Hence providing virus protection for all connected schools was an early priority investment for LGfL, and remains so.

There is however no benefit from this investment if the protective software is not installed and **kept up-to-date** on all devices. For details on how to do this, see [www.SOPHOS.lgfl.net](http://www.SOPHOS.lgfl.net) - a USO login is required.

### **“Option 2” – Raw Internet**

In rare instances, the technical support staff within a school may wish to divest themselves of the security protection afforded by LGfL and make their own arrangements instead. This is strongly NOT recommended but it can be facilitated.

Subject to formal approval by the senior management of the school, expressed through the authenticated authorisation of the Head Teacher, this preference can be accommodated by the reconfiguration of the school's LGfL connection to "Option 2". As with "Category 2", authorisation is given via the Support Site, with the HT's approval automatically generating a support case and setting the process in motion.



The filtering system keeps the children extremely safe whilst accessing the internet. From the point of view of staff the site is easily manoeuvrable with really good links and step by step instructions. I have really gained a lot of experience from raising issues that occur in school and have greatly appreciated the support and feedback from the team at LGfL.  
Southwark Teacher - April 2013.

This option exposes the school's connection to unfiltered Internet access and unrestrained movement of different kinds of data traffic into and out of the school's network. This is not a recommended option but it has been made available to meet the specific requests of a small number of schools. Further information, if required, is available at [www.POLICIES.lgfl.net](http://www.POLICIES.lgfl.net).

### MailProtect - Email filtering

The LGfL StaffMail and LondonMail services include the filtering of all inbound and outbound email, facilitated by the MailProtect service. Email is scanned for unwanted 'spam' emails, viruses, inappropriate language and images. On an average day this system filters more than a million inbound emails, of which typically 25% are categorised as undesirable and are not delivered. This service also protects non-'Option 2' school-hosted email servers.

Additionally, LGfL's 'SafeMail' feature offers schools the opportunity to define rules by which (typically younger) students must use LondonMail when interacting with other users. For example, communications could be restricted to take place only within the school itself or with just a number of approved external domains – with different rules applied to different student year groups.

MailProtect also includes a facility which allows staff users to opt into receiving a nightly email listing the items which were blocked during the previous day and giving the means to release (or 'view' with reduced risk) any which are nevertheless of interest. This service can be switched on within the support site by any staff user, or a school's Nominated Contact can set the option for any staff user in the school.

### Guidance on access to the Head Teacher Portal within the Support Site

Once logged into the support site (accessed via [www.SUPPORT.lgfl.net](http://www.SUPPORT.lgfl.net)) from the 'My Account' drop-down menu, access firstly '**Headteacher Summary**'.

This page gives summary information and allows the Head Teacher to see, and to control, which staff have NC status (doing this online requires an OTP tag to be registered to the Head Teacher's USO account) and, within the context of LGfL services, who can view MIS data, send SMS text messages, and/or approve training course bookings.

Secondly, from the 'My Account' menu, the Head Teacher can access '**Declaration Management**'. Here an HT can give formal approval to one or more options which are accessed from the drop-down 'Declaration' list.

At the time of writing, only the 'Category 2' Remote Access products declaration requires the Head Teacher (and all NCs) to have a USO login plus an OTP tag.

Other Declarations currently include:

- Release of certain elements of pupil data to enable certain LGfL content to operate to maximum effect, for example to provide a gender-specific icon on the screen, or to allow a pupil to save a piece of work within the application.
- Allowing certain devices (printers, cameras) to authenticate against a LGfL WiFi implementation by generic passphrase rather than a personal USO account.
- Allow the use of simplified logins (instead of full USO authentication) - intended to make logging in easier for Early Years pupils.
- Change to 'Option 2' type connection.

A small number of additional authorisations that are HT-specific exist on the Support Site, such as the agreement to automate (or amend) the exporting of MIS data via USO-AutoUpdate.

## Related Questions

### What if I believe the connection is slow?

LGfL 2.0 is a fast, resilient and powerful network. If the school's local network is also well designed, working properly and equipped with relatively modern computers, and provided that LGfL services are configured correctly by the school (notably the WebScreen Internet filtering policies), then the experience at the desktop will be fast and a pleasure to use.

From time to time Nominated Contacts from schools report that 'the connection is slow'. What they are experiencing is a slow response at the desktop, but between the LGfL connection and the user's desktop is the school's equipment.

To check the performance of the LGfL connection, it is necessary to eliminate any intermediate effects by connecting a laptop or other computer directly to the LGfL firewall, while nothing else is connected. (For example, there have been instances where a 'rogue' computer on a school network is broadcasting spurious traffic which is crowding out other traffic.)

Comprehensive guidance on how to undertake a speed test for your LGfL connection is available at [www.SPEEDTEST.lgfl.net](http://www.SPEEDTEST.lgfl.net).

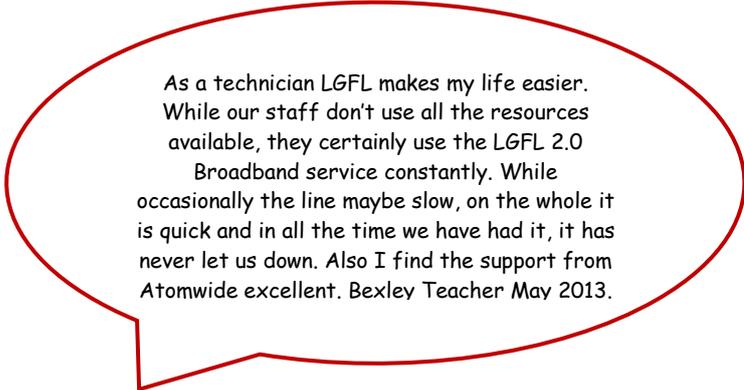
When undertaking a speed test, it must be remembered that even with the firewall isolated there are numerous factors which will impact the result. For example, a speed test completed using a high specification computer will produce a faster result than with a lower specification computer, because it can process the data more quickly. Even a high-spec computer will buffer the incoming data and not achieve a continuous flow. The speed of the equipment at the far end of the test, and how many other users are accessing it at the same time, will also impact the result.

It is also important to understand that when a connection is stated as being, for example, 100Mbps, this is the underlying speed of the connection, not the net deliverable speed of data flow, since some capacity is absorbed in managing the flow of data. Internet traffic, which has to be controlled from both ends of a communication, with data checks and acknowledgements as a series of 'handshakes', is more analogous to road traffic than to water through a hose.

Occasionally a genuine fault does occur, but in the great majority of cases, based on over 10 years' experience of service delivery to thousands of schools, reports of slow performance at the desktop are not usually related to an external fault.

A common explanation of slow performance is that the connection is saturated by the demand for inbound data at peak times within school. This can be investigated by reference to data traffic logging and graphic display which is available for all (non-Option 2) schools within the support site. If a bandwidth upgrade is found to be required, then this can be addressed by raising an order with LGfL at [office@lgfl.org.uk](mailto:office@lgfl.org.uk).

Finally, the Internet itself influences perceived performance, and between certain parts of the world, time zones can play a major part, as can individual websites experiencing atypical demand – the online purchase of Olympic tickets serves as an example of the latter. An example of the former might be UK users accessing US sites and being affected by the host country's business generally 'waking up' at a time that coincides with our own schools' 'lunchtime', with the consequent increase in local demand affecting performance in the UK.



### **What if our connection is not working?**

If your school suffers from a loss of connectivity to LGfL and the wider Internet then an authorised Nominated Contact may telephone the LGfL Service Desk during working hours (8am to 6pm every day throughout the year other than weekends and Bank Holidays) once it has been established that the problems are not local in origin.

On being connected to a Service Desk engineer, the caller will be asked to answer a series of standard questions relating to the LGfL-managed equipment located in the school (it will save time if the state of the indicator/warning lights displayed on this equipment is checked and recorded prior to the initial call). If the equipment is showing as contactable on LGfL's monitoring systems, the caller may be asked to connect a laptop directly to this equipment in order to diagnose any issues relating to the equipment itself or otherwise to confirm that the issue relates to a problem local to the school's LAN.

If the equipment/connection is confirmed as being down on LGfL's monitoring systems then a case will be raised by the Service Desk engineer and escalated to Virgin Media Business for further investigation. Usually, if there is a broken connection, this will have been detected by VMB and will already be receiving attention by their engineers.

### **If my MIS is not supported by LGfL's data extraction process – why not?**

USO-AutoUpdate is the USO 'module' used to automate the creation, management, update and removal of USO accounts in sync with changes to a school's own local Management Information System (MIS).

At the time of writing, five commercial MIS platforms are supported, covering the vast majority of installations in LGfL-connected schools; others continue to be considered for future support. Some MIS products include, and/or successfully support the extraction of, a myriad of data that USO can utilise to personalise as well as secure LGfL and its users. However, other MIS products offer a more limited range of data, and some offer so little (or have so few users) that it becomes economically unviable to author another version of USO-AutoUpdate to support them at all.

In the latter situation, LGfL offers a semi-automated process that aims to support any likely user data export facility, so long as that facility can export the data, preferably on a scheduled and regular basis, via a pre-formatted spreadsheet available from the Support Site.

For establishments without an MIS of any kind, LGfL will accept a template spreadsheet which has been filled out manually. It should be noted that the spreadsheet must be completed for the whole school only (i.e. all staff, all pupils, or all staff and pupils combined).

Spreadsheets submitted manually by schools which could otherwise use AutoUpdate, will be processed manually as soon as time allows, and are subject to processing charges.

### **Can LA or Council personnel still support schools on LGfL 2.0?**

Yes, most certainly. In fact, LGfL welcomes their informed support where available.

However, any LA-level administrators who used to interact with LGfL on your school's behalf will, from the Autumn Term 2013, need to have their role in supporting you explicitly acknowledged by the school to LGfL.

In this way, LGfL is ensuring that the school is always the origin of the audit trail for LGfL support matters, and that only your specifically-appointed external representatives, whether from an LA or a third party commercial support service, can access non-public data about your school, make requests, or intercede in matters on your behalf.

### **Don't you know who I am?**

This question is occasionally addressed vigorously to help desk staff, usually in frustration when none of the appropriately-authorized representatives of the school who have previously been identified to LGfL is available.

From a school's perspective, when the helpdesk declines to take instructions from an unknown person, it is an essential part of securing and safeguarding users and any data relating to them, as well as properly controlling changes that could fundamentally compromise a school's own technical infrastructure. Hence the proper response to the question 'Don't you know who I am?' is likely to be either, "No, but we wish we did, because then we may be able to help you", or "Yes, we do, and we know that you have not been empowered to make this enquiry".

Intrusion detection testing is a standard procedure for any Internet provider, and Service Desk technicians must respond appropriately to any 'testing' of the boundaries (whether technical or in policy). However feasible and justified a scenario for an exceptional response may appear, self-appointment to a role of authority cannot be supported without recourse to checks and balances.

### **In summary**

The personnel charged with supporting LGfL's services and their use in your school, are there to assist you. Their purpose is certainly not to hinder you, but on occasion, in the interests of maintaining proper security and associated procedures, they may appear to, and may even be contractually or legally obliged to.

It nevertheless remains LGfL's purpose, and that of its selected partner suppliers, to serve and support schools, while working to standards required by security policies appropriate to a schools environment. We ask for your understanding and assistance in our pursuit of these goals.

## **What else comes with LGfL 2.0 as well as broadband?**

The launch of LGfL 2.0 brought a new approach to solving schools' needs for online services. Because LGfL is a publicly owned not-for-profit organisation, unlike commercial providers, it is not trying to sell 'extras' to make money. Wherever possible these are simply included as part of the already paid for service.

Sometimes schools are not fully aware and spend money unnecessarily on things which are already available with LGfL so do please make sure you and your team are familiar with what follows.

The LGfL 2.0 service has three main elements:

1. A secure, high speed dedicated broadband connection for each school
2. A wide range of teaching and learning resources and digital collections
3. A carefully designed range of services and support

For information on learning resources please visit [www.WHATS-ON.lgfl.net](http://www.WHATS-ON.lgfl.net) or for the latest developments see [www.SHOWCASE.lgfl.net](http://www.SHOWCASE.lgfl.net).

**The main included service items are briefly summarised below and full details can be found on the Services menu at [www.lgfl.net](http://www.lgfl.net)**

## **E-Safety guidance**

LGfL provides extensive resources and guidance to support schools with the management of e-safety [www.safety.lgfl.net](http://www.safety.lgfl.net)

## **Internet filtering**

Internet filtering is essential to keeping children and staff safe when going online. LGfL's Webscreen 2.0 allows schools to adapt and manage their own filtering policy and includes a facility to apply different policies to different groups of users. Free training is available to Nominated Contacts to support use of this. (See 'Training' below).

## **Industry strength email**

Staffmail, LondonMail and Safemail are high specification services based on Microsoft Exchange and available for all staff and pupils. [www.staffmail.lgfl.net](http://www.staffmail.lgfl.net) : [www.staffmailinfo.lgfl.net](http://www.staffmailinfo.lgfl.net)  
[www.londonmail.lgfl.net](http://www.londonmail.lgfl.net) : [www.londonmailinfo.lgfl.net](http://www.londonmailinfo.lgfl.net) : [www.safemailinfo.lgfl.net](http://www.safemailinfo.lgfl.net)

## **Email scanning**

Email content control scans mail for viruses and inappropriate content and attachments, as well as filtering out huge quantities of unwanted 'spam' email. There is the option of a daily email giving a list of the items filtered out. [www.mailprotectinfo.lgfl.net](http://www.mailprotectinfo.lgfl.net)

## **Unified Sign On**

An LGfL USO for each teacher and pupil is one single username and password to remember for access to all LGfL services and resources, in school, or out. [www.uso.lgfl.net](http://www.uso.lgfl.net)

## **USO FX- Secure File Transfer**

USO File eXchange provides a secure and tracked means of transferring personal or sensitive data between sites (e.g. school to LA) in encrypted format. [www.usofx.lgfl.net](http://www.usofx.lgfl.net)

## **AutoUpdate**

AutoUpdate provides a connection between the school's Management Information System (MIS) and the USO database and keeps the list of LGfL users in your school up to date as new pupils and staff join or leave. [www.autoupdate.lgfl.net](http://www.autoupdate.lgfl.net)

## **Office Apps and Skydrive – shareable online storage**

Each LondonMail account comes with the option of including a large online file storage area and the use of MicroSoft Office web applications.

## **Antivirus protection**

LGfL provides 'Sophos' antivirus protection for all school computers including servers and staff laptops which can also be maintained with updated protection. [www.sophos.lgfl.net](http://www.sophos.lgfl.net)

## Website hosting

Schools can use the LGfL's PLESK platform to host their website. [www.hosting.lgfl.net](http://www.hosting.lgfl.net)

## Video central HD

This is LGfL's own YouTube – a safe area where schools can upload and play video, inserting your own video clips into the learning platform or other locations. [www.vidocentralhd.lgfl.net](http://www.vidocentralhd.lgfl.net)

## Podcasting

Schools can upload their own recordings to LGfL's central podcasting service as a convenient means to publish sound files. [www.podcasting.lgfl.net](http://www.podcasting.lgfl.net)

## Secure Remote Access

LGfL provides RAV3, a software tool which is authorised for use on the LGfL network to provide remote management or access to computers attached to the school network. [www.rav3.lgfl.net](http://www.rav3.lgfl.net)

## CentraStage

CentraStage enables anyone responsible for ICT in schools to manage, maintain, support and optimise their device estate. [www.centrastage.lgfl.net](http://www.centrastage.lgfl.net)

## OpenCheck

OpenCheck provides a cost-free means to quickly communicate site/school status messages to parents, for example when extreme weather forces a school closure. See it in action at [www.opencheck.lgfl.net](http://www.opencheck.lgfl.net)

## Unified Helpdesk

Most service requests are ideally made in writing by one of your school's Nominated Contacts raising a support case on the support site (accessed via the 'blue padlock' icon at [www.lgfl.net](http://www.lgfl.net)) but there is also the option to speak by phone to one of the support team at the helpdesk. There is one number to remember – 020 8255 5555 or for further contact details see [www.contact.lgfl.net](http://www.contact.lgfl.net)

## Network Management and Security

Each school has a secure connection protected by its own dedicated firewall. The helpdesk can assist with any changes in settings which are required to enable new services.

## Training

LGfL supports access to a range of related training opportunities including free training for Nominated Contacts in the use of LGfL services. For more details see [www.training.lgfl.net](http://www.training.lgfl.net)

## What else is available from LGfL?

LGfL offers other optional, not included, services which integrate fully with the existing included services. Some of the more popular include:

### Gridstore

Gridstore provides secure off-site backup for schools' data. Regular automated back-ups eliminate the risks of human error and local unforeseen events. For more details see [www.gridstore.lgfl.net](http://www.gridstore.lgfl.net)

### Internet Telephony

Working with supply partner Atomwide, LGfL can offer a range of IP telephony solutions which save schools money, and give a range of advanced facilities and features, by taking advantage of the high speed LGfL fibre connection.

### Wi-Fi

LGfL in partnership with Atomwide can provide a range of wi-fi solutions which fully integrate into the existing LGfL Internet and authentication services.

For full details of these and other LGfL services please visit [www.services.lgfl.net](http://www.services.lgfl.net)

---

The London Grid for Learning Trust is a company, and registered charity, entirely owned collectively by all London Councils. It was established and incorporated in April 2001 to enable aggregated procurement of broadband and other schools' ICT resources, securing best value through combined purchasing power.

The Trust has a number of specialist governance groups (Editorial Board, Technical Steering Group etc), and operates under an Executive Board populated by Directors of Children's Services and other senior officers. The Chief Executive Officer is Brian Durrant, formerly a teacher and LA adviser/inspector.



## Know your LGfL

---

The main entrance to LGfL	<a href="http://www.lgfl.net">www.lgfl.net</a>
Learn more of what's available	<a href="http://www.services.lgfl.net">www.services.lgfl.net</a>
See the latest content	<a href="http://www.showcase.lgfl.net">www.showcase.lgfl.net</a>
E-safety resources and guidance	<a href="http://www.esafety.lgfl.net">www.esafety.lgfl.net</a>
Keep informed	<a href="http://www.news.lgfl.net">www.news.lgfl.net</a>
See it in action and show your team	<a href="http://www.primary.lgfl.net">www.primary.lgfl.net</a>
See it in action and show your team	<a href="http://www.secondary.lgfl.net">www.secondary.lgfl.net</a>

All of LGfL's services are easy to access and understand as regards to navigating. I really love the fact you have such a wide scope of resources for all key stages within schools. Fantastic you have USO for pupils to use some resources from home too.  
Kensington Teacher - April 2013



[www.lgfl.net](http://www.lgfl.net)

**...making the unaffordable, affordable...**

London Grid for Learning Trust is a consortium vehicle of the London Local Authorities  
A company limited by guarantee registered in England no 4205579 Registered charity no 1090412

Cl Tower St Georges Square New Malden KT3 4TE © LGfL 2013  
help desk 020 8255 5555 tel 020 8408 4455 email [office@lgfl.org.uk](mailto:office@lgfl.org.uk) web [www.lgfl.net](http://www.lgfl.net)