embc

connecting people to learning

WELCOME GUIDE

Setting up on-line services

LONDON GRID FOR LEARNING

TRUSTnet

embc connecting people to learning

Contents

Introduction to embc and LGfL

embc is delighted to have agreed a collaboration with LGfL (The London Grid for Learning Trust) a not-for-profit organisation, owned collectively by a group of 33 local authorities, which provides the London based services to the Education and Public Service sectors.

Under the agreement between embc and LGfL schools are able to purchase the LGfL TRUSTnet suite of services which are delivered and supported by Atomwide Ltd. The services from LGfL TRUSTnet will run over your existing embc Broadband connection.

Purpose of this Welcome Guide

Please read this document thoroughly and well in advance.
This guide aims to assist schools and other establishments in their migration to the LGfL TRUSTnet package of services and any additional services chosen from the options catalogue.. The process is described in detail, including additional explanatory notes appended at the end of the document.

There are numerous references to school-specific situations, but these may apply equally to other sites and should therefore not be disregarded.

A **checklist** is provided at the end of the document to help ensure no step is omitted.

The smooth and successful transition from your current service provider to LGfL's services over embc will require you to prepare for the migration to the new services as well as carry out key setup actions.

There are three phases of transition:

- Pre-installation
- Installation
- Post-installation

There are actions you will need to carry out in each phase.

This Welcome Guide cannot offer a detailed description of every service available through the LGfL TRUSTnet package–references are made to other support resources where relevant, in the text and appendices. Please access these resources to obtain more information and detailed guidance in configuring and using the many facilities available to your school.

Please ensure that this document is provided to all those who are responsible for your site's technical support. You are advised to seek external technical support and advice should an appropriate level of technical knowledge not be available within your establishment.

Step 1: Pre-Installation Actions:

The actions listed here are required by you to prepare your establishment for the migration to the LGfL TRUSTnet services.

Whilst LGfL and Atomwide will be happy to provide advice wherever possible, the preparation for the addition of the LGfL TRUSTnet services can only be undertaken by you.

A useful analogy to describe the move from your existing service to LGfL TRUSTnet would be to compare it to making a domestic purchase of a new refrigerator. When the supplier brings the new fridge to the house, the supplier does not remove the contents of the old fridge and transfer them to the new one. This responsibility is left with the customer.

User accounts

All TRUSTnet services are made accessible via individual user accounts known as USO accounts.
The term **USO** stands for **Unified Sign On**. This account allows users to gain access to every service and resource via the same user credentials.

All staff and pupils in schools subscribing to LGfL TRUSTnet are entitled to a USO user account. This account will be used to authenticate (log into) all services offered by LGfL TRUSTnet itself as well as externally based subscriptions such as teaching and learning resources.

All users will require accounts in due course but initially, during the pre-installation phase, just a small number of key accounts is needed.

Creating the initial user accounts

The two account types needed initially will be:

- Head teacher account
- Nominated Contact account

After registering your school's details and recording your order details via the embc LGfL TRUSTnet registration portal (order.TRUSTnet.pro), **initial USO accounts will be created** for the Head teacher and other key staff.

You will be notified of your account details as follows:

1. An email with the USO account username will be sent to the email address registered for each individual
2. An initial **password** will be sent by text to the mobile phone number provided.

In the event that these account details have not been received within 15 working days of your school's order being entered on the TRUSTnet registration portal, please contact TRUSTnet Customer Services on 020 8255 5555 option 9, or visit www.uso.lgfl.net to access further information.

Head teacher user account

A Head teacher account must be created as this person must then authorise the relevant permissions to be granted to other users, notably to give 'Nominated Contact' status to at least one technical lead, network manager or similar person, as soon as possible

The provision of LGfL TRUSTnet services involves interactions with 'personal data' as defined by Data Protection legislation. The Head teacher in a school has, by default, the role of 'Data Controller' (as defined under the Data Protection Act) and carries with it a number of special responsibilities. However the following should be noted:

1. The vast majority of management tasks in relation to LGfL TRUSTnet are carried out by Nominated Contacts appointed by the Head teacher (see next section and Appendix 1).

2. A number of services which, due to their sensitive nature or security implications, require a Head teacher (in their capacity as 'Data Controller') authorisation in order to be used.

3. A Head teacher authorises such services by logging in to the USO support site (www.uso.lgfl.net) with their USO account and tick a box to indicate that they agree to the activation of those services and recognise the possible implications for the school.

   Examples of such services would be the ability to use the Remote Access service, or automate data exports from the MIS to manage USO accounts for staff and pupils. This authorisation process ensures their activation is with the agreement and understanding of the school at a 'Data Controller' level, and is necessary due to their relevance under the Data Protection Act.

For convenience a Head teacher may elect to delegate the 'Data Controller' role to a senior staff colleague which will then give the latter the authority to authorise the relevant services. There is a form designed for this purpose which may be downloaded from the USO Support Site by a Nominated Contact (see Appendix 1).

Nominated Contact (NC) user accounts

A Nominated Contact (NC) is a user whose account has the permissions to access a range of resources to configure and manage their establishment's service. An establishment can normally have up to five Nominated Contacts.

1. Nominated Contacts are the only users able to access the service support resources, configure service options and obtain assistance relating to any aspect of the LGfL TRUSTnet service.

2. A Nominated Contact can also manage the transition process, via the USO Support Site found at www.uso.lgfl.net

3. A Nominated Contact is created by authorisation from the Head teacher/Principal, or other legal 'data controller'.

4. Only Nominated Contacts can access the online information which is essential to the LGfL TRUSTnet transition process and only the Headteacher or delegated legal 'Data Controller' can authorise the appointment of a Nominated Contact.

It is important that the Head teacher visits the website (www.uso.lgfl.net) to access further information and download a Nominated Contact Submission Form as soon as possible after receiving their USO account credentials. Once completed, the form (or forms – it is recommended that schools have more than one Nominated Contact) should be remitted as indicated on the form.

Further information about Nominated Contacts and the support/management resources available to them can be found in Appendix 1.

The absence of an appointed Nominated Contact will seriously restrict or prevent the processes detailed in the rest of this guide.

Installation of Technical Equipment (Firewall)

When your application for LGfL TRUSTnet services is accepted it will be necessary for a new Firewall to be installed in your school equipment room. This is a straightforward technical installation which takes approximately one hour. There is no disruption to your existing services during the installation.

To complete this Firewall installation a site visit will be required to your school by an LGfL TRUSTnet authorised engineer. The primary contractor for Firewall installation is Virgin Media Business working under instruction and contract with LGfL TRUSTnet on behalf of LGfL.

Rack Space and Power Requirement

Please ensure that there is sufficient space in your equipment cabinet to accommodate the new Firewall equipment that will need to be fitted.

Details of the space needed can be found in the **USO Support Site** by selecting **My Account**, then **TRUSTnet Deployment**, and choosing the **Equipment** tab.

Please note that 1U=1.75 inches or 45mm.

If enough space is not available when the survey is made it is likely to result in your installation being put on hold until you are able to advise that sufficient rack space has been provided.

You will also need to ensure sufficient power sockets are available. Again, the requirements can be found in the **Equipment** tab.

In addition to the equipment and power requirements shown in the Support Site, it is possible that additional equipment requiring an extra 1 U of height in your rack and an additional power socket may be needed.
LGfL TRUSTnet recommend the installation of an Uninterruptable Power Supply (UPS). This is not essential but it

should be considered as an integral part of a site upgrade. If you already have a UPS installed the Firewall should be connected with the UPS.

You should also be aware that the Firewall equipment can be noisy and, in summer, generate unwelcome heat and may be regarded as unsuitable for installation in an office or classroom environment.

Site Documentation

It is vital that your current existing network configuration is documented; this is far easier to do now, while the current systems are working, rather than when these have been migrated to LGfL TRUSTnet. The following is a guide to the information which is essential to a smooth transition. Please ask the person responsible for your IT support to assist you with these details.

Site infrastructure

- IP scheme
- Secure Links to other Networks
- Email and Web servers
- Filtering systems
- Data backup

Any other services you have deployed along with details of the do the provider. If you have services that you provide or manage in house within the school it is important that you also document these.

Other items to consider

- Video surveillance systems
- Security systems
- Cashless catering
- Any system or device that a 3rd party supplier accesses via the internet.

All these details should be recorded by the site and would normally form part of the site Disaster Recovery documentation. This information is going to be invaluable when it comes to connecting to LGfL TRUSTnet.

Enabling services during pre-installation phase

Certain services do not rely on your broadband connection being in place and can be enabled at any time. This will allow your school to :

Set up USO accounts for staff and pupils

USO accounts can be created and maintained by several methods:

1. A Nominated Contact may create a single account at any time via the USO Support Site http://support.lgfl.net. From here, access the User Accounts tab, select User Request (Single) and fill in the online form.

2. While not recommended, USO accounts may be created for a whole school request by submitting a spreadsheet. A pre-configured spreadsheet template is available to download from the Support Site. Output from a Management Information System (MIS) such as SIMS can be imported into this spreadsheet template and the file uploaded via a dedicated page on the support site. More details on how these techniques work are to be found in the online Support Site User Guide. (See Appendix 1 for 'Accessing the online Support Site User Guide')

3. The very much preferred method for creating and updating user accounts is to use AutoUpdate software which is available at no additional cost. This is designed to operate in conjunction with a school's MIS to export data on a regular basis (normally overnight). This exported user data is then used to create, modify, transfer and delete USO accounts assigned to the school.

   a. Using AutoUpdate significantly reduces the time involved in managing hundreds of accounts manually.
   b. AutoUpdate provides far more accurate user data than is possible through other means.
   c. AutoUpdate automatically tracks school population changes (joining and leaving staff, for example) so that USO accounts are created and removed in a timely fashion.

More particularly there are some LGfL TRUSTnet services where the use of USO-AutoUpdate is an essential pre-requisite. Schools are advised always to implement the necessary USO-AutoUpdate technologies where a supported MIS is installed.

It is strongly recommended that an early review is made of the detailed description of USO-AutoUpdate and how it may be implemented in various MIS environments. This can be found in section 17 of the Support Site User Guide.

Transitioning websites to LGfL hosting

Webhosting is included at no additional cost as part of the LGfL TRUSTnet service.

- You may use either an IIS (Microsoft) or Apache (Linux) resilient platform with a 15GB limit per site. If you require more space please raise a support case to discuss.

- To make use of the LGfL TRUSTnet web hosting service please raise a support case and ask for it to be enabled. You will receive details on how to access your web space.

The web hosting service may be set up and activated in advance of the installation of the physical connection but not before the Nominated Contacts have been created (see the earlier **Nominated Contact (NC) User Accounts** section of this Welcome Guide).

Externally hosted sites

It is possible that your school website is hosted (stored) 'in the cloud' (i.e. on a remote web server rather than on a server on your local network). If so, the transition to LGfL TRUSTnet will not affect your access to it.

However, if your website is hosted with your current internet service provider (ISP) it may cease to exist when you disconnect from their services. Therefore, please ensure you move it to the LGfL TRUSTnet platform before the end of your existing contract.

You will need to know the following details:

- Who it is hosted with
- Who controls and manages the domain name (most important)
- Who designs and updates the website

Internally hosted sites

Establishments that run their own internal web site servers and wish to continue to do so, only need to raise a support case via the USO Support Site http://support.lgfl.net (see Appendix 1) and request an internal IP address to be mapped to be a real world IP (a 'MIP' or managed IP address).

The MIP request is made by submitting a spreadsheet. A template designed specifically for this purpose can be downloaded from the LGfL deployment area on the Support Site. Access the My Account tab, select LGfL deployment, and then choose the **Firewall and Mail Relay** tab (Appendix 2). The domain DNS settings would then be changed to reflect the change of the real world IP address.

Mail Services

Establishments migrating services to LGfL TRUSTnet are likely to have existing mail services which may or may not be linked to the previous ISP.

LGfL TRUSTnet offers two mail services: one designed exclusively for staff users called StaffMail and another for pupils called TRUSTmail. The steps required to set up these services are described later in this section.

Hosting your own mail server

If your school hosts its own local mail server (for example, a Microsoft Exchange system) then the internal IP address of the server will need to be mapped to be a real world IP (a 'MIP' or managed IP address) and the relevant ports opened to allow it to be accessed.

This is done by raising a support case via the USO Support Site http://support.lgfl.net with the request. The DNS would then be changed to reflect the change of the real world IP address.

You will also be joining the MailProtect email filtering system and a request should be made to enable the filtering of inbound mail for the school-based server. This is based upon the domain hosted on that device.

If this work is carried out in advance of the installation then careful timing will be required for switching the settings on the day of the installation itself. Please make sure the Support Desk is aware of your requirements and timetable to make the transition as smooth as possible. Advice and guidance can be obtained by raising a support case or by telephone to assist with any aspect of the transfer process.

If your current mail system is hosted 'in the cloud', is not dependent on your current ISP (and thus will not be terminated along with their services), and will be retained after the move to LGfL TRUSTnet then it will be important to make sure that your web filtering rules (in WebScreen 2.0) are configured to allow access once the site has moved onto the LGfL TRUSTnet service. Advice on filtering is available later in this document.

Setting Up StaffMail

To enable StaffMail for your school a Nominated Contact must:

1. Raise a support case via the USO Support Site (see Appendix 1) and request the StaffMail service to be enabled.

2. In the same support case, the Nominated Contact should request Mail Domain Admin rights to be applied to their USO account.

   Please note that these rights should be requested even if you don't wish to host the school domain on the StaffMail system as these rights will allow the Nominated Contact to access the management tools on the Support Site for the StaffMail service.

Once the service has been enabled, the Nominated Contact with Mail Domain Admin rights can manage mailbox accounts. Mail accounts can be created for all staff users by:

1. Enabling each one individually, or
2. Through a bulk request.

These processes are documented in detail in the Support Site User Guide (see Appendix 1), in sections 8.2 and 8.4 respectively.

Users who have had StaffMail accounts enabled can access the service in two ways:

1. The webmail interface is available at https://mail.LGfLmail.org

2. A dedicated locally installed client may be used. (Outlook is recommended for PC users though any mail client capable of accessing an Exchange-based mail service should be suitable – this includes mail clients on a variety of mobile devices).

   It should be noted that not all features in StaffMail are available in all client interfaces – the Service Desk can provide advice if required.

Email addresses based on your school domain can also be supported within StaffMail – if this facility is required then a request should be made by raising a case on the USO Support Site. The Service Desk will be able to provide advice on the best way to migrate the school's domain and how to do so with the minimum inconvenience to users while the migration is taking place.

There is a large amount of detailed information on how to configure StaffMail and make the best use of its many additional features in the Support Site User Guide (see Appendix 1).

Setting Up TRUSTmail

To have TRUSTmail enabled for your school a Nominated Contact will need to raise a support case via the Support Site (see Appendix 1) and request the TRUSTmail service to be enabled. The case will be updated once this has been done.

- Once the accounts are set up then they can be accessed via a dedicated link on www.LGfL.net (In the top right part of the screen.)
- Pupils use their USO account details to log in when prompted for their credentials.

The TRUSTmail service is hosted by Microsoft Office365. It gives staff and pupils access to other Office365 services, such as OneDrive and web-based Office apps (Word, Excel and PowerPoint), which are provided to staff and pupils as part of the LGfL TRUSTnet service.

Further details on how to make these services available to your users can be found in Section 8.3 of the Support Site User Guide (see Appendix 1) or contact the Service Desk for help.

Please note that although the Service Desk staff can provide advice on migrating the contents of existing mail services and mailboxes to one or more of the mail systems offered by LGfL TRUSTnet it is not possible for them to carry out any migration of data contents on your behalf.

Sophos Anti-Virus

Sophos Anti-virus software is supplied as part of your LGfL TRUSTnet subscription. It can be downloaded and installed on all workstations and servers within the school during the pre-installation phase if wished – in fact; it is recommended that schools do so.

Sophos may be installed as a standalone product on individual workstations and servers or its distribution can be controlled from a single server using Sophos Enterprise Console. The latter offers a simple and more efficient means to manage large numbers of devices through a single interface so is recommended for all but the smallest schools.

Please note that, before you attempt to install Sophos, you are advised to remove any previous anti-virus product that may have been installed on your workstations and servers. As with many anti-virus product, Sophos does not operate effectively alongside other anti-virus products so their removal is an essential step before installing Sophos.

Detailed instructions for installing and configuring both Enterprise Console and standalone versions are available in the Support Site User Guide.

Once in the Guide, select "installing EC <version number>" in section 14 if you plan to install the Enterprise Console. Step by step instructions for installation are provided.

> *If you are installing Enterprise Console before migrating to your LGfL TRUSTnet services connection you will need to enter your USO account details when configuring the updating settings for the console. When you have migrated on to your LGfL connection you can remove these details as authentication will be based upon the IP address of the server.*

If you are installing standalone versions please choose the appropriate instructions for either PC or Mac. Once again, follow the step by step installation instructions and remember to enter your USO details in the updating configuration settings if your school is not yet connected to LGfL TRUSTnet.

As with other services provided by LGfL TRUSTnet, advice and support are available via the telephone support line or through a case raised on the USO Support Site. Please do not hesitate to contact the Service Desk via either route if you require assistance.

Step 2: Installation Actions:

Commissioning

This part requires interaction with both your staff AND network

Following installation of the firewall during the same visit, you will need to witness several simple tests to demonstrate the new service is working and confirm a record of this. This will be via a sign-off sheet presented to you by the authorised LGfL TRUSTnet engineer.

Once signed off, the service can have the schools network connected by the school nominated contact when all necessary preperations have been compleated.

Change necessary network settings

Implement the changes you made preparations for in the Pre-Installation Actions above.

If necessary contact the person responsible for your ICT support to accommodate the specific requirements of your site's local area network.

Important note: Your embc private IP range remains the same. No changes are required to provide the standard set of LGfL TRUSTnet services.

However, a change will be required if your school has any servers publicly visible to the Internet, for example a local webserver. If there are mapped internal IP addresses to a public IP address a new public IP address will be provided.

Neither LGfL TRUSTnet nor its supply partners can provide free-of-charge site visits to support sites with the bespoke settings or configuration of their local network or networks, which can vary widely. If a site visit is required the service is available at a rate of £90 per hour.

Step 3: Post-Installation Actions:

1. Configure internal services - this may include Proxy Servers, e-mail addresses, IP addresses, etc.

2. Test to ensure all services are accessible and access rights are set correctly. Any issues should be raised through the USO Support Site www.support.lgfl.net

3. Upload website content – if not completed prior to the transition put into action arrangements to transfer website content (See page 8 of this guide).

4. Record that the new network environment configuration is correct and has been tested.

Services to be enabled Post-Installation

WebScreen 2.0 filtering management

By default, as soon as your school is connected to LGfL TRUSTnet services it will be subject to default embc filtering policies which define access to all websites outside the school's own network.

These policies have been designed to provide a level of filtering that attempts to balance the requirements of schools to access the maximum number of sites with the minimum of inconvenience. The default rules block access to certain content categories that most schools would wish (and indeed expect) to be denied to their pupils.

All default filtering policies can be amended by a filtering administrator in your establishment.

It is recognised that a "one size fits all" approach will not suit many schools (the initial policies are fairly strict) so there is a large degree of flexibility available to schools to modify the policies to suit local needs and levels of supervision.

The WebScreen 2.0 management interface is found in the USO Support Site.

> It permits filtering administrators to modify existing policies and create additional ones. Policies can be modified by allowing or blocking whole categories, individual sites or even keywords. Administrators also choose how, when and to whom each policy is applied.

In order to manage the school's filtering, one or more Nominated Contacts will require additional permissions.

> The permissions to be a "filtering administrator" can be requested by simply raising a case on the USO Support Site and specifying which users require these rights.

These rights will give access to the full range of WebScreen 2.0 management functions. An extensive list of options will appear in the USO Support Site under the WebScreen 2.0 button.

Instructions and advice for school-level management of the WebScreen 2.0 filtering system are available online via the Support Site User Guide. Free training courses take place at Atomwide's offices in Orpington on a regular basis. Details of upcoming courses can be found at http://www.events.LGfL.net.

Remote Access – RAv3

LGfL TRUSTnet offers all staff in your establishment the ability to remotely access resources located inside your network (i.e. to access school machines from home).

This is accomplished by a set of tools collectively referred to as RAv3 which is based upon industry-standard Cisco remote access technologies and hardware.

To make use of this technology at your establishment:

1. The Head teacher (or appointed delegate) must log into the USO Support Site access the **Service Desk** tab and then choose **Remote Access resources** from the menu.

2. The Head teacher must tick the box to **Enable RAv3 access for this school**.

3. After the service is enabled, a Nominated Contact will have full access to configure the service. This is done in the USO Support Site by selecting Service Desk followed by Remote Access Resources.

4. Full instructions on configuring this resource and an explanation of the various configuration options are found in the Support Site User Guide (Section 13).

LGfL TRUSTnet has categorised other, third party, remote access products into three categories. Some pose potential security risks and are discouraged or proscribed – for further information on remote access and the various options visit www.policies.lgfl.net and download the **LGfL Security Guidance** document.

Appendix 1: Nominated Contact Basics

Logging on to the USO Support Site

Open a browser, go to www.support.lgfl.net and click on the blue padlock. This will take you to a page where you must enter your USO account details (user name and password).

Raising a case on the USO Support Site

The process of requesting help from the Service Desk is always referred to as "raising a support case" and is done via the Support Site where a full history and audit trail is then stored.

1. Log into the Support Site as described above.
2. Click on the **Service Desk** tab
3. Select **Raise an Issue** from the menu.
4. Follow the steps required on each page (fill in the online form)
5. You will be required to choose a Topic for the case from a list and provide a description of the issue you are raising.
6. Any time your case receives an update, an email will automatically be generated to the person who raised the case. Emails will be sent to the email address which has been registered to your USO account.

When a case is concluded you are invited to close the case on your own initiative. If a Support Desk staff member believes that the issues raised in case have been resolved then an "Intent to Close (ITC)" status update will be applied. The case will then be closed automatically if either of the following conditions is met:

1. The case has not been updated for 30 days following the posting of the ITC
2. The case has not been updated for 2 working days after the person who raised the case has read the ITC.

Seeking advice by phone

You will be required to raise a support case online if you need the Service Desk to make any changes. However, if you simply need general advice on technical and service matters this can be provided via the telephone support line – call 020 8255 5555 and select option 3 to speak to a support engineer. You may be advised to raise a case on the matter being discussed if, for example, a more detailed investigation of an issue is required (particularly where the case needs to be escalated to engineers at various levels and occasionally representing different organisations) but many issues can be resolved without such a step being required.

Accessing the online Support Site User Guide

The Support Site User Guide documents the functionality available in the USO Support Site. To access the Guide, a blue button in the top right corner of the Support Site will take you to the documentation regarding the page from which the Guide is accessed. You can always use the menu on the left to select a different topic when needed.

Creating a new user account via the Support Site

New user accounts can be created manually, online, at any time.

> *Please be aware if that user is going to be recorded in your MIS and your school is exporting data from the MIS directly you do not need to create accounts manually. In such situations, any user recorded in the MIS should automatically have an account created for them by the following day.*

To create an account:

1. Log in to the USO Support Site as described previously.
2. Click on the **User Account** tab
3. Select **User Request (single)**.
4. Fill in the appropriate fields marked with a red asterisks.
   Although the mobile number field has no asterisk, it is very important that this is filled in as it enables the automation of secure password delivery.

After the form is submitted you should receive an email stating the new USO account has been created. The newly created user's details can be checked following this confirmation by accessing the **User accounts > User list/search** section within the Support Site.

Delegation of Data Controller status

If the Head teacher wishes to delegate data controller rights and responsibilities to another senior member of staff then please log in to the Support Site, and from the **Resources** dropdown menu, select **Forms** and click on the **Headteacher Proxy Authorisation Form** link.

Second factor authentication (OTP tags)

OTP tags are small devices, designed to be attached to a key ring or similar, which enhance security by providing second factor authentication when accessing certain key services and websites. This means that in addition to a username and password, the user will need to enter a code generated by the device.

> For example, the USO Support Site not only contains a large amount of potentially sensitive data (including user details of both staff and pupils) but also has within it a number of pages that allow Nominated Contacts to manage key LGfL TRUSTnet hosted services.
> For this reason schools are advised to consider purchasing OTP tags for its key account holders (Nominated Contacts and possibly the Head teacher). This means that any individual with a registered OTP will have to log in using both their login credentials and a code to access key sensitive data and resources.
>
> Such second level authentication has become more common in recent years – banks, for example, employ similar techniques using specialised devices to provide enhanced security for their users.

While OTP tags are not mandatory, their use is recommended and there are a small number of services where they may be required in order to enable some specific configuration that are deemed to have a higher security risk than more standard settings.

> An example would be enabling access to some external web-based remote access services under the terms of the **LGfL Security Guidance** document outlined in the section earlier in this document about **Remote Access – RAv3**.

Training Courses provided by LGfL TRUSTnet

Free one-day training courses are run on a regular basis for Nominated Contacts and provide practical advice and help with managing the main services provided by LGfL TRUSTnet. There are also more specialised courses that cover the main features of the WebScreen 2.0 filtering system and how to manage the system at school level to provide the most effective and flexible filtering of web sites.

These courses are run by Atomwide and are free to attend in their specialised training facility in Orpington, Kent.

Details of forthcoming courses can be found at http://www.events.LGfL.net and by accessing the **Training** tab on the USO Support Site.

Appendix 2: The LGfL TRUSTnet Deployment Area

How to access the LGfL TRUSTnet deployment area on the Support Site and update key information

1. Open a browser, go to www.support.lgfl.net and log in by clicking on the blue padlock and entering your USO user name and password on the authentication page.
2. Click on the **My Account** dropdown menu and select **LGfL TRUSTnet deployment**.
3. If necessary select your site from the drop down lists.

You will then see a number of tabs: **Overview, Contacts, Virgin Media, IP Addresses, Firewall and Mail Relay, Equipment, Documents, FAQ**.

These tabs give all the information that is held about your site. Please check this information for accuracy and omissions as this could impact upon your final installation.

- The **Overview** tab provides a summary of the key information relating to the deployment of the LGfL TRUSTnet service.

- The **Contacts** section lists the key contacts for the school and their respective roles. This needs to contain the relevant people to be contacted regarding the installation.

- The **IP Addresses** page provides a summary of the IP address ranges allocated to the site.

- The **Firewall and Mail Relay** section provides a summary of any special MIPs which have been implemented as well as specified Firewall settings applied to the site.

- The **Documents** page contains electronic versions of key documents, including the sign-off document completed during installation

- The **FAQ** section contains a large number of questions and answers relating to the more technical aspects of the LGfL TRUSTnet service. Technical staff supporting schools are advised to read this section carefully.

Appendix 3: Checklists

Checklist: Pre-installation actions

The following describes a number of areas in which the site management must ensure action.	✔
Check your site has at least two Nominated Contacts registered on the LGfL TRUSTnet Support Site.	
Existing services may hold information which should be recorded, in advance of transition.	
■ Current Network Configuration	
■ Domain Name	
■ Website, Hosting and Creator	
■ Secure Links to Other Networks	
■ Email Providers	
■ Filtering: Any Particular Internet filtering policies which the site has set up and wishes to retain will need to be documented ready for re-establishing in the new filtering system.	
■ Hosting of MS Exchange and Website (MIPS)	
■ Data Backup	
■ 3rd-Party Support Providers	
Content	
Domain Name Server settings	
IP Scheme	
Key staff should read all online LGfL TRUSTnet service literature to familiarise themselves with new or different features, particularly the new Internet filtering system.	
The person mainly responsible for supporting ICT should attend a free one day training session hosted for LGfL TRUSTnet by Atomwide in Orpington – please see www.events.lgfl.net	
Existing VPN (Virtual Private Network) arrangements must be notified by raising a support case.	

Checklist: Installation Day actions:

Commissioning	
Witness simple tests to show the new service is working and confirm a record of this.	
The equipment fitted will include a new firewall which will be configured and managed for LGfL TRUSTnet by Atomwide. This will usually be completed by remote online access to the firewall.	
Implement the changes you made preparations for in the Pre-Installation Actions above.	

Checklist: Post-installation actions:

Specific activities	
■ Configure internal services, e-mail addresses, IP addresses, etc.	
■ Tests should be undertaken to ensure all services are accessible and access rights are set correctly.	
■ Upload website content – if not completed ahead of transition put in-hand arrangements to transfer any website content to LGfL hosting.	
■ If remote access to the site network is required, raise a support case for the RAv3 secure remote access service. Other remote access products are discouraged or proscribed on LGfL. Cisco RAv3 is supported and is included at no additional cost.	
■ Request access for the management of the site's Internet filtering policies by raising a support case by going to www.support.lgfl.net	
■ When access has been granted, the site's Nominated Contact should manage the policies by logging into the Support Site and first consulting the on-line manual. You are strongly advised to attend one of the free Nominated Contact training courses which covers the topic of web filtering in some detail - details available from www.events.lgfl.net	
■ Test the site's filtering policies	
■ Record your testing	