

Best Practice Guide CLEO Remote Access Services

A Guide to Preparing Your School Network & Remote Users PCs

V 4.2

Published: 03 April 2006

Please refer to www.cleo.net.uk
for the most recently published version



1 Index

1	Index	2
1.1	Other Relevant Documents	2
2	Introduction - Managing the Technical Challenges & Risks	3
2.1	Development of this Best Practice Guide	4
3	Recommended Specification for School Servers and Remote PCs	5
3.1	School Server Minimum Specification	5
3.2	Remote PCs Minimum Specification	5
4	Recommended Configuration for School Network	6
4.1	DNS and DHCP Recommendations	7
4.2	Securing Wireless LANs	7
4.3	Network Administrator Passwords	7
5	Monitoring usage & performance	8
6	Best Practice Guide to Setting up User groups	8
7	Preparing a client PC	8
7.1	Recommended PC/OS Specs	9
7.2	Client Configurations	9
7.2.1	Operating system updates	9
7.2.2	Anti-virus software (installed and updated)	9
7.2.3	Personal Firewall (installed and active)	10
8	Remote Users Group Policies	11
8.1	Remote Access VPN + RDP users policies	11
9	Where to Seek Further Advice	20

1.1 Other Relevant Documents

The following list includes all documents and forms required for the CLEO remote access services. Please ensure you have read all documents relevant to the service you require:

Documents relevant to all services:

- Introduction to CLEO Remote Access Services – A Short Guide for Headteachers and Senior Managers
- Introduction to CLEO Remote Access Services – A Detailed Guide to the Benefits and Risks for Headteachers and Senior Managers
- Best Practice Guide to Preparing Your School Network and Remote Users PCs
- CLEO Remote Access Services Terms & Conditions, and Acceptable Use Policy
- Initial Enquiry Form

Documents specific to individual services:

- Technical Guide – Setting Up RADIUS
- Technical Guide – Setting up CLEO VPN
- Technical Guide – Setting up CLEO Web Gateway
- Technical Details Submission Form – available online for each service

2 Introduction - Managing the Technical Challenges & Risks

One of the strengths of the CLEO network is the protection it provides all schools connected to it, as they are part of a private network with strict security in place to protect all schools from viruses, trojans and security breaches wherever possible. However by opening the network to remote users, to meet the needs of schools in the region, instantly increases the risks to individual schools and their PC networks. With this in mind CLEO offers its remote access services to schools on an annual renewable basis and after schools have worked with their respective LA ICT Support services to ensure their schools networks are prepared for remote access. All initial applications are made through the LAs so they can discuss the issues with your school's ICT staff at an early stage.

We strongly recommend that you implement the guidelines contained in this document, in particular with reference to the network diagrams and information described in section 4. These setups have been successfully demonstrated as good examples of structuring your network for use with CLEO remote access services.

It is important to recognise the risks by enabling remote access to your school network and from an early stage. Key risk areas include:

Risk / Issue	Probability of occurrence	Management of risk
Difficulty in ensuring that remote users apply security advice and take appropriate measures to protect the schools network while working remotely	High	Specifically, CLEO VPN should only be used on remote users PCs that are owned and/or managed by the school . CLEO VPN should not be installed on personal home PCs
Network security – risk of unauthorised access by users unknown to CLEO network or schools	High	All school networks to employ best practice in security, defining remote user group access rights separately, ensuring all servers and remote PCs are up to date with system upgrades, fixes and patches. CLEO core systems will log access by remote users for security purposes. Logs will only be analysed by site for statistical purposes, but records of access by individuals e.g. date, time, site, IP address will be stored for recall for security breach purposes only (see privacy statement in “Terms & Conditions”). Remote PCs using the CLEO VPN service to have personal firewall enabled – also recommended for CLEO Web Gateway. CLEO reserves right at all times to suspend remote access services.
Viruses attack network	High	All servers and PCs to have anti-virus software installed and systems put in place to ensure all software is up to date and that fixes are applied
Best practice recommendations not followed by schools	Medium	Schools must work with LA ICT support services at an early stage and ensure they adhere to guidelines – service only offered on school year cycle, before school has to reapply. Schools must ensure that their IT staff are confident in implementing the service as defined by CLEO.
Software Licensing	Medium	Additional software licences may be required for

		remote PCs. Schools must check licensing arrangements for any software used from home.
Management of remote users	Medium	Who and when? Use of timed access periods to prevent issues such as interference with network backups etc
Improperly secured wireless networks, either in school or at home	Medium – High	We strongly recommend that CLEO remote access services are NOT used with wireless networks unless appropriate authentication and encryption are in place, especially when used in conjunction to access sensitive data such as admin networks. Schools must ensure appropriate measures are implemented.

2.1 Development of this Best Practice Guide

This guide addresses some of the practical and technical issues that were identified during the pilot of the VPN solution. It describes:

- The recommended approaches to preparing your school network
- Required policies and optional policies
- Recommendation for setting and managing remote users PCs
- Common problems and their solutions

It is not a detailed “How to Set Up Remote Access” – please refer to the relevant technical guide for each service.

3 Recommended Specification for School Servers and Remote PCs

The following lists the **minimum** specifications that CLEO know will work effectively for enabling remote access via each service to your school network. CLEO and both Lancashire ICT support and Cumbria CC ICT Support should be able to provide advice and support for schools wishing to implement remote access based on these minimum specifications (see also configuration section).

For all other specifications both CLEO, its network providers and the LA ICT Support Services are only able to offer support based on best endeavours and cannot guarantee to help your school establish a remote access service. If this applies to your school, please consider whether the chosen service is essential to your requirements. You may be able to meet the requirements of your school using an alternative approach e.g. deploying the CLEO Web Gateway solution or for website hosting, by using the website hosting services offered by each Local Authority.

3.1 School Server Minimum Specification

The minimum recommended specification for school servers to operate each service across CLEO is:

For the CLEO VPN solution:	Windows 2003 or greater, either with or without ISA server
For the CLEO Web Gateway solution:	Any currently supported Microsoft operating system, providing automatic updates are available. (When in Internet Explorer, go to “Tools/Windows Updates” and install the “Critical Updates” feature. Linux or similar, providing they are regularly updated

All servers must have a firewall in place.

3.2 Remote PCs Minimum Specification

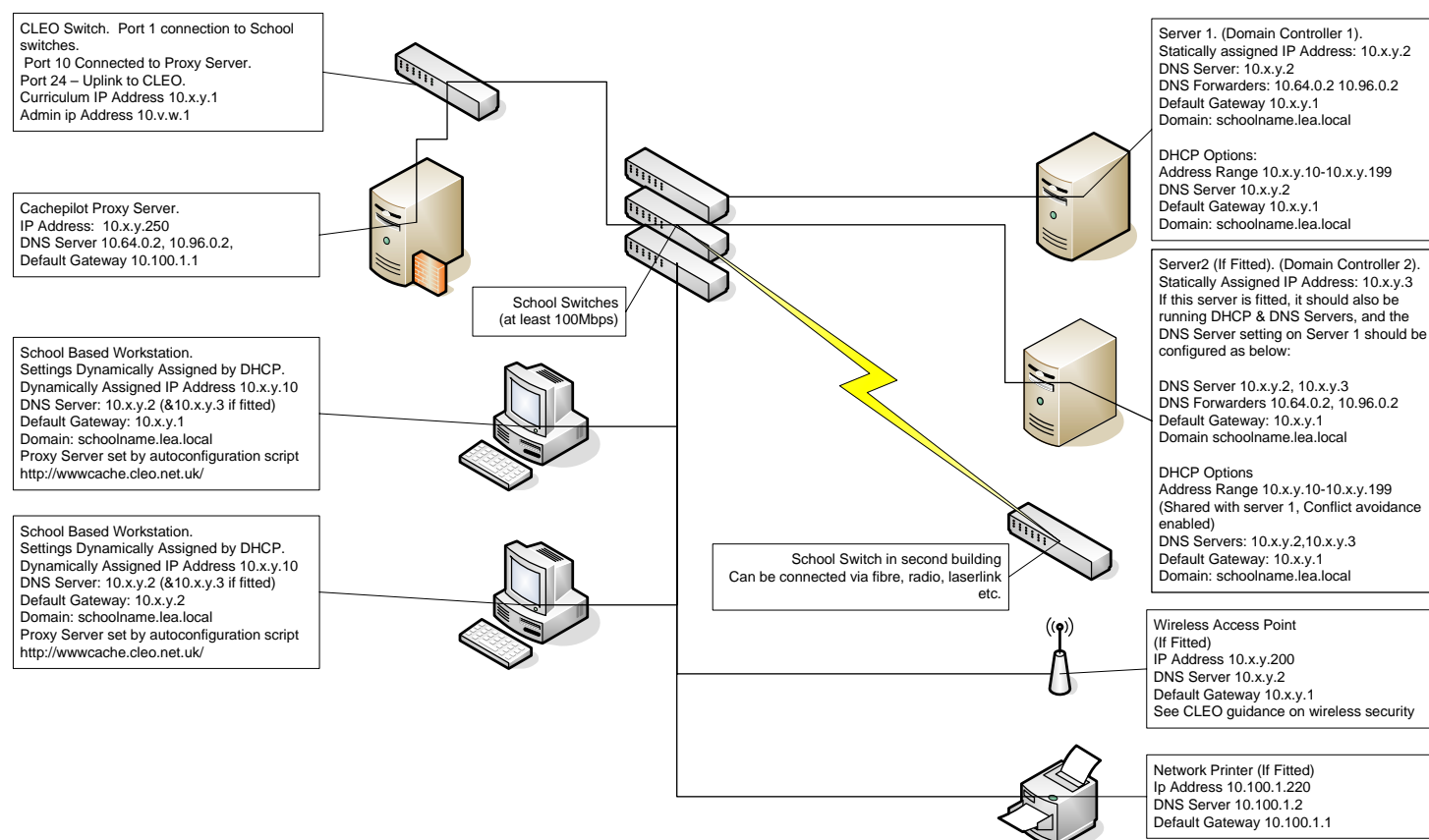
The minimum recommended specification for remote users PCs is:

For the CLEO VPN solution:	Minimum Windows 2000Pro, MS Windows XP Home or Pro operating systems
For the CLEO Web Gateway solution:	Any recent browser

4 Recommended Configuration for School Network

Many of the challenges in successfully establishing a remote access service to your school network across the CLEO network relate to ensuring the school network is designed and configured correctly. As a result of the trials carried out with the original pilot the following configuration is provided as an example of good practice when setting up the school network. This configuration should ensure that the remote access service will work and that it is setup securely:

Network Settings, Network Attached to CLEO



4.1 DNS and DHCP Recommendations

These are a few pointers on setting up a Windows 2000 or 2003 domain at a CLEO connected site. Windows Active Directory is not entirely reliant on DNS for its correct operation: if you get your DNS configuration wrong on either of your servers or client PCs a range of very strange faults can occur. For extra fun these can be intermittent and transitory.

1. Have two domain servers acting as Domain Controllers and also have DNS installed.
2. Do NOT use your Internet domain name as your windows domain name. This will cause headaches if you ever want to do remote access. e.g. use <schoolname>.<LEA>.local in place of <schoolname>.<LEA>.sch.uk
3. The DNS service should be configured for Cumbria schools to forward all other enquires to the CLEO DNS servers 10.96.0.2 & 10.64.0.2. For Lancashire schools the settings are as follows: DNS 212.219.82.4 and secondary DNS 212.219.83.4
4. DHCP is a good idea for client PCs but ensure at the DHCP DNS settings are for your internal Windows DNS servers only.
5. Static Addresses are a good idea for servers - make sure your static DNS settings are for your internal Windows DNS servers only.

These points are particularly important if you are running a firewall like MS ISA or Censor-Net box.

4.2 Securing Wireless LANs

As part of the process of setting up your school network you should also take into account security of wireless LANs. Whether or not you are enabling remote access at your school it is essential that wireless LANs are properly secured. Please ensure you adhere to the security recommendations and instructions provided by the manufacturer of the equipment. You may also wish to refer to the BECTA website and the JANET website for helpful guidance and a range of useful reference documents:

<http://www.becta.org.uk/corporate/corporate.cfm?section=8&id=146>

<http://www.ja.net/development/wireless/nw-admin.html>

Please remember that it is **essential** that you provide advice to staff to help them secure home wireless access points before enabling CLEO VPN remote access. If you have any doubts about how to set up your wireless network securely please contact your Local Authority Schools ICT Support Service for advice.

4.3 Network Administrator Passwords

Security of passwords is absolutely essential in designing a network to follow best practice principles. The following guidance should always be adhered to:

- Network administrators must **never** login in over remote access links using the administrator password, including from another PC within the school.

- High level users usernames must **never** identify themselves as high level users e.g. “bob-admin”
- Network administrator passwords and other essential passwords should be stored securely, preferably in the school safe.
- Passwords should follow guidelines for creating strong passwords. See the Microsoft website for more information:
<http://www.microsoft.com/athome/security/privacy/password.msp>

5 Monitoring usage & performance

An important part of the pilot was to evaluate the level of use, periods of high demand, how the service was used, etc... Use of the service will continue to be monitored by CLEO for security and performance purposes.

The level of monitoring will be as follows:

Recorded	Purpose	Stats
Successful authentications	Determine usage	<input checked="" type="checkbox"/>
Unsuccessful authentications	Aid support groups, security	<input checked="" type="checkbox"/>
Client information (OS, etc...)	Aid support groups	<input checked="" type="checkbox"/>
Duration, start, end of connection	Determine usage	<input checked="" type="checkbox"/>

Key: recorded not recorded

Statistical information developed from monitoring will not identify individuals, and may be made available from the CLEO web site.

6 Best Practice Guide to Setting up User groups

Careful consideration should be made of which users are provided with remote access and when. For ease of support both within individual institutions, it is recommended that access is provided in a staged fashion. This sort of rollout should allow any issues to be resolved with end users, by providing them with support in a controlled way.

A typical rollout might be as follows:

- School ICT Technicians and Network/System Administrators
- ICT Coordinators, IT motivated and experienced users
- Staff issued with machines maintained/managed by school

6.1 Essential Recommendations for Remote Users

Remote access using the VPN solution **MUST NOT** be set up on remote users personal PC equipment – ***please restrict use to school owned PCs or Laptops for Teachers PCs.***

Please ensure you include the following advice for remote access within your schools ICT acceptable use policy:

For security reasons, staff must not access any of the remote access services from a publicly accessible PC such as a library or internet café based machines.

In addition the pilot demonstrated that the VPN solution is generally considered unsuitable for pupils and therefore it is also strongly recommended that pupils are not given VPN access. A new web interface solution is currently being developed to specifically address the requirement for pupil access to school networks. If your pupils will only need access to a school hosted VLE we recommend the CLEO Web Gateway solution instead.

For more information on recommended user groups, please refer to the “Technical Guide to Setting Up RADIUS”

7 Preparing a Client PC

Having prepared the servers within your institution to support remote access, then remote client PCs also need to be prepared. The following are some best practice guidelines.

7.1 Recommended PC/OS Specs

It is recommended for each remote access service that a remote PC should be home broadband connected (minimum 512K ADSL broadband) and be running Windows 98, 2000 or XP.

To protect your institutions network and that of CLEO any PC being used for remote access must have comply with the following:

7.2 Client Configurations

The following requirements are also defined within the CLEO Remote Access Services Terms & Conditions and Acceptable Use Policy.

Enforcing such requirements when the PC is not on the premises of an institution requires careful consideration. Schools should develop suitable administration and management procedures to ensure that staff, teachers and/or pupils accessing facilities in the school using remote access are adequately supported and have sufficient information to minimise the risks involved. All remote users **must agree to follow the acceptable use policy** and security guidelines.

7.2.1 Operating system updates

The operating system of all remote PCs must be kept patched and updated (Windows Update and Windows Software Update Service), to ensure it is protected against known exploits and ensure the most stable platform possible. See **Windows Software Update Service** guide.

7.2.2 Anti-virus software (installed and updated)

Both Local Authorities have licensing deals with Sophos that allow teachers and support staff to install Sophos Anti-virus on school PCs and Laptop for Teachers PCs at no additional cost. An install package configured to automatically update from outside of the CLEO network will be made available. See the **“Installing Sophos Anti-virus on a Standalone PC”** guide available from your Local Authority ICT Support service.

7.2.3 Personal Firewall (installed and active)

It is recommended that all PCs connecting to the internet through an ISP have a personal firewall installed. For Windows XP users this can be easily be achieved by apply Service Pack 2 and configuring the Windows Firewall. However the Windows Firewall is quite basic, it only inspects inbound packets to determine whether they are solicited or unsolicited. Solicited packets are allowed through, unsolicited are dropped. This is adequate protection for a clean system, but if a Trojan or virus has already established itself on the system then it will still allow the virus to broadcast itself. There are many other firewall solutions available, with much more sophisticated features. Often these are available from Anti-virus vendors such as Symantec.

8 Remote Users Group Policies

The following grids illustrate recommendations for remote users and remote computers policies:

8.1 Remote Access VPN + RDP users policies

If you are enabling either remote desktop or terminal services with your school domain, the following policies will help reduce risks associated with these services:

DOMAIN

[hide all](#)

Computer Configuration (Enabled) hide	
Windows Settings hide	
Security Settings hide	
Account Policies/Password Policy hide	
Policy	Setting
Enforce password history	6 passwords remembered
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
Account Policies/Account Lockout Policy hide	
Policy	Setting
Account lockout duration	30 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	30 minutes
Local Policies/Audit Policy hide	
Policy	Setting
Audit logon events	Success, Failure
Administrative Templates hide	
Network/Network Connections/Windows Firewall/Domain Profile hide	
Policy	Setting

<u>Windows Firewall: Allow ICMP exceptions</u>	Enabled
Allow outbound destination unreachable	Enabled
Allow outbound source quench	Enabled
Allow redirect	Enabled
Allow inbound echo request	Enabled
Allow inbound router request	Enabled
Allow outbound time exceeded	Enabled
Allow outbound parameter problem	Enabled
Allow inbound timestamp request	Enabled
Allow inbound mask request	Enabled
Allow outbound packet too big	Enabled
Policy	Setting
<u>Windows Firewall: Allow local program exceptions</u>	Enabled
<u>Windows Firewall: Allow remote administration exception</u>	Enabled
Allow unsolicited incoming messages from:	[domain controllers]
Syntax:	
Type "*" to allow messages from any network, or else type a comma-separated list that contains any number or combination of these:	
IP addresses, such as 10.0.0.1	
Subnet descriptions, such as 10.2.3.0/24	
The string "localsubnet"	
Example: to allow messages from 10.0.0.1, 10.0.0.2, and from any system on the	

local subnet or on the 10.3.4.x subnet,
 type the following:
 10.0.0.1,10.0.0.2,localsubnet,10.3.4.0/24

System/Group Policy[hide](#)

Policy	Setting
Internet Explorer Maintenance policy processing	Disabled
User Group Policy loopback processing mode	Enabled
Mode:	Merge

System/Remote Assistance[hide](#)

Policy	Setting
Offer Remote Assistance	Enabled
Permit remote control of this computer:	Allow helpers to remotely control the computer
Helpers:	administrators

Policy	Setting
Solicited Remote Assistance	Enabled
Permit remote control of this computer:	Allow helpers to remotely control the computer
Maximum ticket time (value):	1
Maximum ticket time (units):	Hours
Method for sending e-mail invitations:	Mailto

Windows Components/Windows Messenger[hide](#)

Policy	Setting
Do not allow Windows Messenger to be run	Enabled

[Do not automatically start Windows Messenger initially](#)

Enabled

Windows Components/Windows Update[hide](#)

Policy

Setting

[Allow Automatic Updates immediate installation](#)

Enabled

[Configure Automatic Updates](#)

Enabled

Configure automatic updating:

4 - Auto download and schedule the install

The following settings are only required

and applicable if 4 is selected.

Scheduled install day:

0 - Every day

Scheduled install time:

09:00

Policy

Setting

[No auto-restart for scheduled Automatic Updates](#)

Enabled

[installations](#)

[Specify intranet Microsoft update service location](#)

Enabled

Set the intranet update service for detecting updates:

http://sus0.cleo.net.uk

Set the intranet statistics server:

http://sus0.cleo.net.uk

(example: http://IntranetUpd01)

User Configuration (Disabled)[hide](#)

Windows Settings[hide](#)

Internet Explorer Maintenance[hide](#)

Connection/Automatic Browser Configuration[hide](#)

Policy

Setting

Automatically detect configuration settings

Disabled

Automatic Browser Configuration

Enabled

Interval	Every 10 minutes
Auto-config URL (.INS file)	
Auto-proxy URL (.JS, .JVS, or .PAC file)	http://wwwcache.cleo.net.uk/

URLs/Important URLs [hide](#)

Name	URL
Home page URL	http://www.cleo.net.uk/
Search bar URL	Not configured
Online support page URL	Not configured

RDP

[hide all](#)

Computer Configuration (Enabled) [hide](#)

Administrative Templates [hide](#)

Network/Network Connections/Windows Firewall/Domain Profile [hide](#)

Policy	Setting
Windows Firewall: Allow local port exceptions	Enabled
Windows Firewall: Allow Remote Desktop exception	Enabled
Allow unsolicited incoming messages from:	[Curric 10.x.y.0/z],[Admin 10.x.y.0/z],[remote 10.x.y.0/z]
Syntax:	
Type "*" to allow messages from any network, or else type a comma-separated list that contains any number or combination of these:	
IP addresses, such as 10.0.0.1	
Subnet descriptions, such as 10.2.3.0/24	
The string "localsubnet"	

Example: to allow messages from 10.0.0.1,
10.0.0.2, and from any system on the
local subnet or on the 10.3.4.x subnet,
type the following:
10.0.0.1,10.0.0.2,localsubnet,10.3.4.0/24

Policy	Setting
Windows Firewall: Protect all network connections	Enabled

System/Group Policy[hide](#)

Policy	Setting
User Group Policy loopback processing mode	Enabled
Mode:	Merge

Windows Components/Terminal Services[hide](#)

Policy	Setting
Allow users to connect remotely using Terminal Services	Enabled
Always show desktop on connection	Disabled
Deny log off of an administrator logged in to the console session	Enabled
Do not allow local administrators to customize permissions	Enabled
Remove Disconnect option from Shut Down dialog	Enabled
Restrict Terminal Services users to a single remote session	Enabled

<u>Sets rules for remote control of Terminal Services user sessions</u>	Enabled
Options: No remote control allowed	
Policy	Setting
<u>Start a program on connection</u>	Enabled
Program path and file name	http://www.cleo.net.uk/remotearr/tcs.html
Working Directory	

Windows Components/Terminal Services/Client[hide](#)

Policy	Setting
<u>Do not allow passwords to be saved</u>	Enabled

Windows Components/Terminal Services/Client/Server data redirection[hide](#)

Policy	Setting
<u>Allow audio redirection</u>	Enabled
<u>Allow Time Zone Redirection</u>	Disabled
<u>Do not allow client printer redirection</u>	Enabled
<u>Do not allow clipboard redirection</u>	Disabled
<u>Do not allow COM port redirection</u>	Enabled
<u>Do not allow drive redirection</u>	Enabled
<u>Do not allow LPT port redirection</u>	Enabled
<u>Do not allow smart card device redirection</u>	Enabled
<u>Do not set default client printer to be default printer in a session</u>	Enabled
<u>Terminal Server Fallback Printer Driver Behavior</u>	Enabled
When Attempting to Find a Suitable Driver:	Do nothing if one is not found.

Windows Components/Terminal Services/Sessions[hide](#)

Policy **Setting**

Set time limit for disconnected sessions

Enabled

End a disconnected session

5 minutes

Policy **Setting**

Sets a time limit for active but idle Terminal Services sessions

Enabled

Idle session limit:

30 minutes

Policy **Setting**

Sets a time limit for active Terminal Services sessions

Enabled

Active session limit :

2 hours

Policy **Setting**

Terminate session when time limits are reached

Enabled

User Configuration (Enabled)[hide](#)

Administrative Templates[hide](#)

Windows Components/Terminal Services[hide](#)

Policy **Setting**

Sets rules for remote control of Terminal Services user sessions

Enabled

Options:

No remote control allowed

Policy **Setting**

Start a program on connection

Enabled

Program path and file name	http://www.cleo.net.uk/remotearr/tcs.html
Working Directory	

Windows Components/Terminal Services/Client[hide](#)

Policy	Setting
Do not allow passwords to be saved	Enabled

Windows Components/Terminal Services/Sessions[hide](#)

Policy	Setting
Allow reconnection from original client only	Disabled
Set time limit for disconnected sessions	Enabled
End a disconnected session	5 minutes

Policy	Setting
Sets a time limit for active but idle Terminal Services sessions	Enabled
Idle session limit:	30 minutes

Policy	Setting
Sets a time limit for active Terminal Services sessions	Enabled
Active session limit :	2 hours

Policy	Setting
Terminate session when time limits are reached	Enabled

9 Where to Seek Further Advice

Technical support for the CLEO remote access services is provided by each of the Local Authority ICT School Support Services. All requests for CLEO remote access services are coordinated through these services – if you have any queries during the setup process and preparation of your network they will be able to provide advice. Please note that, although the CLEO remote access services are free and the LA Schools ICT Support Services will advise you on the settings required they may charge for any additional work requested to assist you in preparing your network.

Cumbria Schools

Jeff Haslam

Tel: 07967-050356

Email: jeff@cict.org.uk

Lancashire Schools

The Westfield Centre

Tel: 01772-623222

Fax: 01772 621209

Email: callcentre@westfield.lancsngfl.ac.uk