

Managing School networks and file servers

A guide for Primary schools

Produced By:	Leonard Veenendaal Technical Services Manager
Reviewed By:	Dave Ager
Team:	ICT Technical Services
Date:	January 2007
Version	1.6

Contents

Contents	2
Management Summary	3
Support.....	3
Security	3
Access to information	3
Connectivity.....	3
Policies and Planning	3
Managing school networks and file servers.....	4
Network Services	4
Different types of networks	5
Typical Primary schools admin/slave network	5
Typical Primary school server-centric network.....	6
Managing a school network.....	7
Support.....	7
Security	8
Access to data and applications	9
Shared Resources.....	9
Information Management.....	9
Cabling.....	9
Internet Connection.....	9
Policies & Plans	10
What about “master” and “fileserver” computers?.....	11
<i>What to expect from an Education ICT Service supplied and installed server</i>	11
Contact.....	11
<i>Annex A - Sample network configurations</i>	12
<i>Annex B - Managing a “Peer” network</i>	13
<i>Annex C - Network Administration & Advice and Guidance</i>	14
Additional related areas & documents for Information.....	16

Management Summary

School networks have grown dramatically in size and importance over recent years. The principal drivers for this change have been the growth of educational resources in the curriculum and the increasing need for school leaders and administration staff to share information. The network is now a key part of the school's infrastructure and the networked PC has become an indispensable part of the school environment.

The rapid change in role and status of the school network means that there has not necessarily been a similar growth in the understanding and management of the system. This guidance aims to provide some necessary background, raise issues of management and provide pointers to sources of information and expertise available to the school. It also covers a range of management needs from the operational (keeping the network going) to the strategic (how the network will develop and how this is reflected in the ICT development plan).

The main areas for consideration are:

Support

- What are the critical parts of the network and are they adequately supported? Are staff aware of how to deal with any problems that may arise? Does the school have access to good quality advice on specific issues?

Security

- Are critical parts of the infrastructure adequately protected from physical damage or other attack (e.g. computer viruses)? Is data properly protected under the terms of the Data Protection Act? Is there an appropriate disaster recovery plan?

Access to information

- Do staff and students have adequate access to the information and resources they require to do their job or carry out their studies? What solutions have been deployed to prevent access to inappropriate content and information?

Connectivity

- Does the network meet current needs and how should it to develop to meet future needs?

Policies and Planning

- What are the overall management needs and who is accountable for them? Are they reflected in school policies and plans? Are adequate resources devoted to development, training and asset replacement?

Managing school networks and file servers

All schools now have a computer network and the complexity of these varies considerably. As the school's network grows and develops, teachers and managers need to understand what this means for the school and how best to manage the changes and the technology. This guidance is intended to help schools understand the functionality and management issues involved with their school network and file server.

Network Services

Network services are the capabilities that networked computers share. Numerous combinations of network devices, computer hardware and software provide network services.

What is a basic network?

This is actually quite a difficult question to answer. However, this guidance assumes that the school has anything from 2 to 50 computers that can be connected in some way to the school's network system. As a consequence, the computers can share some resources, most commonly email and Internet access. Annex A at the end of this guidance illustrates some of the common network setups.

Computer networks are often classified as one of the following two types:

- **Peer-to-peer Networks**

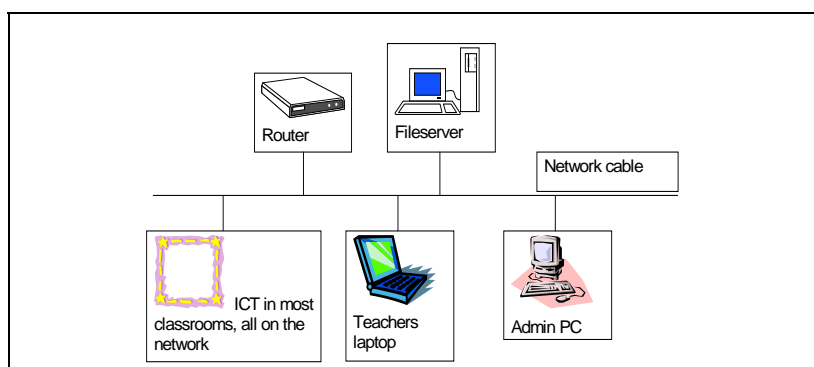
Peer-to-peer networks allow any entity to both request and provide network services.

Most schools started out with a simple "peer" network. As time passed and resources permitted it was then added to. For a number of important reasons, DfES are encouraging schools to have combined or whole school networks. The CCN broadband network and cabling projects has delivered this to Cambridgeshire schools. Some of the reasons for these changes are set out in "Room For Learning 2", published by the ICT Service. As peer networks are fast disappearing, there is a small section in Annex B about them.

- **Server-centric**

Server –centric networks involve strictly defined roles. By definition a server-centric network allows for the server to manage the network security, what users are allowed to do on the computer and what data they are allowed to see or access. Server-centric networks are the recommended and preferred network solution for schools.

Many schools will be working towards a network similar to the one illustrated below, though the fileserver might still be the "Master" machine in the office.



Different types of networks

You may hear a lot of technical terms in talking about networks – “peer to peer”, “master/slave”, “fibre optic”, “fileserver”, “router”, “switch”, “CAT5e”, “wireless” and many others. With a few exceptions, there aren’t many reliable definitions, so this guidance makes its’ own and explains each term as it is used.

Access to data and applications

Issue/requirement		Help and advice
All the admin computers need access to the central data store. The Master machine “acts” as a file server. Do all the admin computers need access to the central store? If not, then it will be important to know which will and which will not and manage them separately.	Admin /slave network ✓	As part of the cabling and networking project, schools will have received advice on how this works.
The network setup must ensure that each computer user can only use the applications and files they are entitled to. User IDs and passwords determine user access.	Server - centric ✓	The school will have to set up systems to administer users’ access and rights. Good practice in user administration is set out in Annex C. Further technical advice should be sought from Education ICT Service or any other suitably qualified service provider.
If the system is intended to store files for more than 10 admin staff, or used for storing both admin and curriculum data & files, then a master computer will not be appropriate, as it is not designed for this purpose.	Server-centric ✓	Technical advice should be sought from Education ICT Service or any other suitably qualified service provider.
You may want some or all of your “curriculum” computers to be able to access your admin system (for example, for assessment software) because they’re in the classroom where the teachers are most of the time.	Server-centric ✓	Specific advice using Windows Active Directories (AD) policies & profiles should be sought from Education ICT Service or any other suitably qualified service provider.

Typical Primary schools admin/slave network

Networks that have “master” and “slave” computers typically are modelled on the “master machine” having the central SIMS installation and the slave Dinner Money or other finance package. Backups are normally performed from the master machine. These networks are accessed by admin/teaching staff and are separate from the curriculum network. This guidance therefore calls them “Admin/slave” networks. Admin/slave networks where all the computers are more or less equal can be categorised as “peer” networks. (Annex B contains more information about this type of network)

Typical Primary school server-centric network

These networks will have a dedicated file server on which all admin and curriculum data and files are stored. Centralising files on a file server not only simplifies administration, it helps maintain consistency of shared data files. When changes are made to a shared file, they become available to all users immediately. Servers have a tape back up device capable of backing up considerably more than a floppy, zip or CD drive and all the data and files are centrally backed up on the server. User IDs and passwords determine user access. This means that the administrator will typically configure admin/teaching staff permissions to access both admin and curriculum areas on the server (if needed). Pupils only have access to the curriculum data and can even further be defined to year groups or only the users own files. All Windows 2000 or higher computers that are connected to the server will be prompted for a user ID and password when logging on. A security policy of what that user is allowed to do on the network or on that specific machine is then distributed from the server, removing the need for Winsuite or similar programs. At the same time the computer will update with the latest anti-virus protection. Anti-virus, policies and profiles are all configured and managed centrally from the server eliminating the need to update and configure each individual computer throughout the school, greatly simplifying network administration.

Advantages of a file server

- Files can easily be shared between users.
- A file server is easy to backup as all the data is stored in one place.
- Policies and Security managed centrally from the server - users cannot see other users' files unlike on stand-alone machines. **Note: Subject to client machines being Windows 2000 or higher**
- Sophos anti-virus is centrally managed from the server automatically updating all PCs on the network, removing the need update each individual machine.
- SIMS and other MIS software can be centrally installed on the server allowing staff (for example, for assessment software) to access it from any school computer. **Note: Subject to client machines being Windows 2000 and the SIMS client installed on the computer**
- SIMS and other MIS software centrally installed maximises the use of remote support reducing the need for on-site technical support.
- Network software licences are likely to be cheaper than buying several stand-alone licences.

Disadvantages of a file server

- Purchasing a file server can be expensive.
- Managing and maintaining a fileserver can be complicated and will require some technically trained support.
- If the file server breaks down none of the computers can access any data held on the server. The computers would still have Internet access. Staff laptops would have offline access.

Addressing the disadvantages

- For schools that already have an ICT Suites or PC's in each classroom and want to extend the network as a 'next phase', a fileserver maximises the return on the investment in PCs and the network infrastructure.
- Education ICT Service or any other suitably qualified service provider, offer various levels of affordable support through SLA's¹. Education ICT Service SLA's include remote support reducing the need for on-site technical support.

¹ <http://www.ictsla.cceducation.net>

Managing a school network

Admin/slave networks that have “master” and “slave” computers have many of the same management issues as a server-centric network with a dedicated fileserver.

Support²

Once the school sets up a server-centric network, support for particular aspects of the network becomes a much more significant issue. Over time these pass from being just “useful” to being “essential”, so for example, the router becomes a critical piece of equipment. Similarly, if the master or fileserver computer breaks down the school will probably need it working again quite quickly.

Issue	Help and advice
<ul style="list-style-type: none">• What are the really important parts of the school's network?	Possibilities are the router and any central storage like a fileserver. Include other equipment that may be critical like LCD projectors and interactive whiteboards.
<ul style="list-style-type: none">• What support arrangements does the school have for these items?	How long can the school manage without one of these items working? If the school's staff cannot support them properly you will need external expertise in the form of a support contract with Education ICT Service or any other suitably qualified service provider. The need to get things working again has to be balanced against affordability.
<ul style="list-style-type: none">• Are the school's staff aware of the support arrangements and do they know how to get support and what to expect?	Make staff aware. Procedures need to be documented in the staff handbook or similar guidance for staff.

Some important resources will be stored on the school's server, particularly the pupil, teacher and finance data in the school's Management Information System (MIS). There are key issues to address:

Issue Identified	Risk / Potential Impact	Advice & Guidance
Physical Security	Downtime or loss of data	Make it as difficult as possible to steal or damage the server. Placement of the server should be a high priority, the location should well ventilated, have adequate network connectivity and be reasonable secure to protect this computer from fire, theft, flood, etc.
Backup	Downtime or loss of data	With the increasing amount of data in schools systems, this needs to be effective. Backups should include all the data in the MIS plus other important files like Word documents and Excel spreadsheets. Historically backups went onto floppy disks however, they are very unreliable, and are not suitable in today's ICT setups an alternative backup systems should be investigated. Ideally an automated system should be used that runs overnight and doesn't rely on someone to start it off. Annex C gives further advice.
Data Protection	Data loss, unauthorised disclosure\access or damage	The Data Protection Act requires holders of personal data to take reasonable steps to protect data from loss, damage or unauthorised disclosure. If the school is going to make parts of its MIS available through the network, then it has to ensure there are good electronic systems (usually user IDs and passwords) to protect it and that staff know the procedures and use them. Annex C gives further advice.

³ <http://www.ictsecurity.cceducation.net>

Access to data and applications

- Identify which computers need particular applications. Set out a procedure for making sure each copy of a given piece of software is upgraded at the same time.
- Make sure your network security is robust and all software on the network is licensed (see Annex C)

Shared Resources

- Identify the activities for which you are planning to use the network. Apart from online resources, think also about other resources that could be shared such as printers and files, videoconferencing and mobile IT, such as laptops and PDAs.

Information Management

With time, your school will have increasing amounts of information on its network – pupil records, teaching resources, pupil's work.

Issue	Help and advice
<ul style="list-style-type: none">• How will this information be stored efficiently and securely?	Avoid the use of floppy or ZIP disks and USB memory sticks as the only storage. Make use of the network as the 'official' store and use other media to transfer work between school and home.
<ul style="list-style-type: none">• How will the school's network enable users to find information quickly?	Establish a simple policy for storage of files i.e. filer naming conventions
<ul style="list-style-type: none">• How will pupil records be adequately protected?	See Annex C on network security.
<ul style="list-style-type: none">• What if the "server" breaks down?	Make sure there is a suitable warranty and support agreement in place (see section on Support on page 6/7)

Cabling⁴

All schools will have received advice as part of the cabling and networking project. The following are included as a guide for when schools are discussing their network cabling needs.

- Are there enough connections in the right places?
- Cable runs need to be as short as possible (technical and health and safety reasons)
- Remember that computers need electricity as well as network cables – you may need to have extra power as well as network sockets
- Wireless is an extension of your network and not a replacement.

Internet Connection

This has been taken care of as part of the CCN and cabling and networking projects. However, it's now crucial to your school's ICT strategy and must work reliably.

- Keep up-to-date with developments in the CCN and cabling and networking projects. Full details are available from www.icttid.cceducation.net > [Schools CCN Information and Guidance](#)

⁴ http://c9s.e2bn.net/e2bn/leas/c99/schools/c9s/web/public/Techsupport_team/info/webpages/tid/Broadband/CCN.htm

- The Broadband network is supported by NTL. The Education ICT Service will take responsibility for logging problems that arise with network connectivity, and will ensure adequate levels of support are maintained.
- Ensure your "As Build" documentation, supplied to your school as part of the CCN migration, is kept up to date. This is an essential tool for maintaining and supporting your network. The document should be stored in a safe, but central location, where it can be easily amended by responsible members of staff
- Make sure your Internet, email & network security policy is up to date and used by everyone in the school, including helpers and governors.

Policies & Plans

All schools will have an ICT Development plan, either as a separate plan or part of the school's Improvement Plan. Extensive guidance on ICT planning can be found on the schools portal under Management / School Leadership. Issues that are specific to the school's network are listed below

- The school's ICT plans should reflect current and projected use of the school's network(s).
- Networks represent a significant investment for schools. The school will need a process to keep up-to-date with changes and to plan an effective development strategy for the school's network.
- Policies – identify (a) who will be accountable for the day-to-day running of the school's networked systems, (b) who will be overall accountable for the operation of the school's Management Information Systems (probably SIMS) and (c) who will be accountable for ensuring curriculum network requirements are met.
- Training - identify training requirements for staff at all levels. This includes regular technical training for in-house school technicians.
- Asset replacement - ensure there is an effective asset replacement plan to upgrade or replace ICT equipment throughout the school over an appropriate timescale.
- ICT equipment is vulnerable to opportunist theft therefore all equipment should be located in rooms which are kept locked or failing that secured by a high security cable or similar to an immovable object

What about “master” and “fileserver” computers?

For most practical purposes, a master computer is not very different from a dedicated fileserver. The principal difference is that a fileserver is much better designed and built than a desktop computer and has additional features like a tape drive for backup. Components of a computer specified as a File Server are produced to more stringent standards, and are therefore generally more reliable, with a greater mean time before failure. Performance and reliability is often increased in a server by including some or all of the following: • Faster, self-checking memory • Redundant power supplies • An uninterruptible power supply to protect against power spikes and power cuts • Fast (SCSI or SAS) hard drives which can be configured in RAID arrays to help reduce the likelihood of data loss through hardware failure • Dual core processors to increase performance • The server should not be used for any other purpose and is often treated like a ‘black box’ – it just sits there handing out files and data to other computers on the network and managing security. It may even be locked away in a cupboard and only have its tape changed once a day.

The main differences are summarised here:

	Master	Fileserver
Backup method	Often manual	Automatic – often overnight
Backup media	Often CD Rom, DVD RW ZIP disk or similar	Usually magnetic tape
System backup	Often data only	Whole system
The computer is switched off overnight	Often	Never
I have to log on to the computer as it starts up	Maybe	Yes
I can use this computer just like any other workstation	Yes	No
If there is a problem in the school's network (e.g. the cabling), can school staff (or pupils) get to their files or SIMS?	Only the master machine will work.	Depends on where the problem is

What to expect from an Education ICT Service supplied and installed server

Only quality best value hardware with a mandatory 3 years onsite service (Currently same business day 4 hour response time).⁵

The server specification and build is carried out and technically vetted by qualified trained senior Education ICT Service technician.

Design always takes into consideration the uniqueness of the school and implemented in with professional project approach.

All school server installations include a standard package which includes the following:

Setup - All Servers are set up exactly the same, following a standard set of instructions.

Installation - Server is installed and has two follow-up visits to check for 'teething problems' & ensuring staff understands how the new system works, and is comfortable with it.

Systems - Every File Structure, policies and pupil logon are standard across all schools, contributing to the ease of administration and support.

Documentation - All Schools receive documentation of system configurations, explaining how their new system works and also provides crib-notes for day-to-day tasks.

Contact

For more advice about planning, installing or managing file servers and school networks, please contact ⁶:

Leonard Veenendaal

Technical Services Manager

Leonard.Veenendaal@cambridgeshire.gov.uk

Education ICT Service, 42 West Street, Godmanchester, Cambridgeshire PE29 2HJ

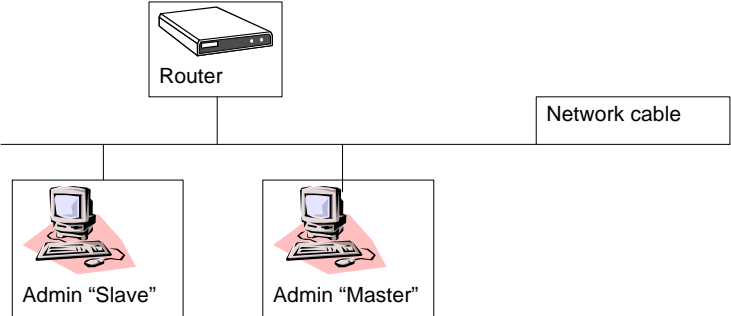
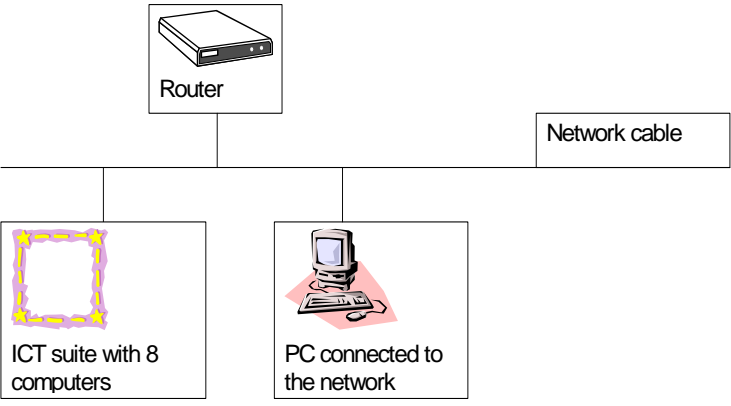
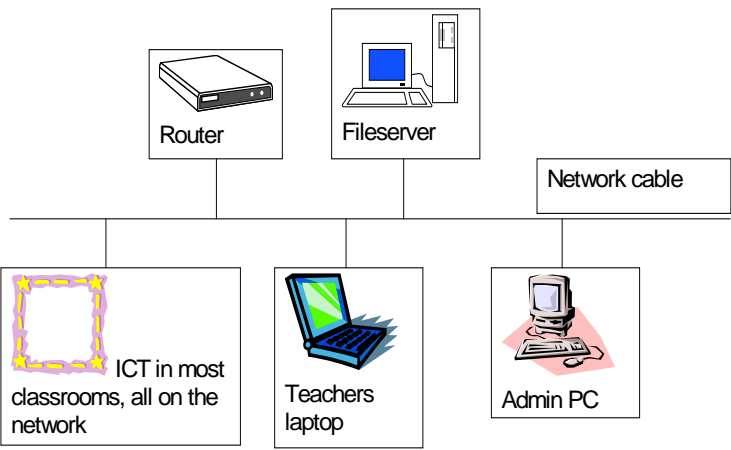
Tel: 01480 376655 Fax: 01480 376660

⁵ <http://c99.e2bn.net/e2bn/leas/c99/schools/c9s/web/public/Procurement%20team/Index/about/>

⁶ http://c9s.e2bn.net/e2bn/leas/c99/schools/c9s/web/public/Techsupport_team/info/webpages/team.htm

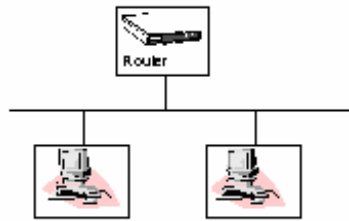
Annex A - Sample network configurations

The following pictures illustrate some of the possible types of network in schools.

 <p>Router</p> <p>Network cable</p> <p>Admin "Slave"</p> <p>Admin "Master"</p>	<p>Typical "Admin peer" network. Cabling connects computers to the network. A router provides the connection to the internet</p>
 <p>Router</p> <p>Network cable</p> <p>ICT suite with 8 computers</p> <p>PC connected to the network</p>	<p>Typical "curriculum peer" network. There's an ICT suite and a few computers elsewhere in the school that are connected to the network</p>
 <p>Router</p> <p>Fileserver</p> <p>Network cable</p> <p>ICT in most classrooms, all on the network</p> <p>Teachers laptop</p> <p>Admin PC</p>	<p>More advanced whole school network. The school has purchased a dedicated fileserver on which the admin data (e.g. SIMS), teachers' and pupils' work files can be stored.</p>

This is not a definitive list – it is intended to show the kinds of networks schools have used, and there are many variations on these themes.

Annex B - Managing a "Peer" network



This is the simplest kind of network. None of the computers have any special role on the network and they probably all have their own printer. The running of the network depends largely on two technical issues: Is the cabling OK? And is the router working?

As far as pupils' and teachers' files are concerned, you can either use the computer's hard disk for storage or use floppy disks. Files stored on the hard disk can only be accessed on that computer unless you deliberately copy them elsewhere or make the file available through sharing it. It may be necessary to create folders where each user or each group of users can store their work. Care is needed to prevent work accidentally being deleted or over-written. Files stored on floppy disks can be taken anywhere (even home), but are susceptible to loss and damage. Virus protection is advisable if users are bringing in floppy disks from home.

Advantages of peer networks:

- Easier to set up
- No real day to day management
- Much less expensive than dedicated server networks
- Spread the burden of providing services over many computers

Disadvantages of peer networks:

- Less secure
- More difficult to manage effectively
- Harder to back up all network resources
- Higher-end network applications may require a network operating system (such as Windows 2000 or 2003 Server) on which to run
- Clients that also provide services to others may perform more poorly
- More query traffic on the network effectively slowing your network down

Annex C - Network Administration & Advice and Guidance

Under the Data Protection and Freedom of Information Acts, schools have a duty to take reasonable steps to protect the data they hold on staff and pupils. This guidance is written largely with that in mind. It is not intended as a step-by-step guide to operational network management.

Network setup

- Disable Guest and anonymous user accounts.
- Anti-virus software should be on the network and all machines and there should be processes to ensure it's kept up to date. Sophos anti-virus is available to all schools subscribing to the core SLA⁷.
- Like all computers on a network, ensure that your server has the required level of service packs and security hot fixes
- Ensure that all users have an ID and password. Passwords should be unique. If you intend using "group" IDs for whole years or other pupil groups, you will need to create appropriate "group" areas on the network for shared files.
- Ensure each ID can only gain access to the parts of the network they are permitted to use. No pupil account should be able to use MIS like SIMS or Dinner Money or "see" any part of the system (including the workstation's hard disk) that might enable them to do this.
- Internet access. As a general rule, computers in the "curriculum" have more restricted access than "admin". Make sure all staff is aware of the difference - for example a teacher's laptop might well be used in the classroom, but may well be connected to the "admin" side of the network.

User administration

Account management, security and Passwords

The following advice and guidance has been put together by the Education ICT Service and as a result of the internal audit review by Audit and information Governance.

Generic accounts remove the audit trail for activity against the account. If a user shares a username with any other user, it will not be possible to identify which user performed which actions. This would cause problems should a security incident need to be investigated. Primary schools should give equal consideration to network security as that expended by secondary schools. Primary schools need to consider not just the risk of security breaches due to pupils (which could be considered to be low) but also due to staff and other network users. It should be possible to trace every network user's actions and to limit the access of each user of school ICT equipment.

- All staff must use individual usernames and passwords when accessing the network. Do not share your password with anyone else.
- In the case of pupils this is not considered practical, therefore the use of a year group or class logon provided that user group is routed through the E2BN Protex 8082 (Middle) CCN default transparent filtering level is applied.
- When staff (or pupils) leaves, delete their old account and issue a new one – don't be tempted to "recycle" IDs. In the case of staff accounts, move key files to whom ever takes over the role.
- Choose a quality password of at least six characters.
- A good quality password will be easy for you to remember and will incorporate other numbers and characters, for example 98.My.Pet (Don't use this password!). Avoid using obvious passwords such as just your pets name, "teacher" or your children's names

- Memorise your password rather than writing it down. Don't tell anyone what it is.
- If your password becomes compromised change it immediately.
- Make sure you change your password(s) every 30 days.
- User accounts should be caused to time out after a defined period of inactivity. (e.g. the school screensaver gives a time-out after ten minutes). When teaching a lesson the consideration could be to set the time out to the duration of the lesson.
- Given that a username is a starting point for an intruder using brute force techniques to be able to crack an account password schools should use group policy to cause the user account to lock after five failed login attempts.
- Knowledge of the Domain administrator password should be limited to the Head and (where necessary) the ICT coordinator. Changing the password at intervals is recommended, particularly if the password has become more widely known. (If your school has a file server support SLA with Education ICT Service please contact us regarding domain administrator password changes).
- Ensure that the PC is logged off when not in use. During the day when a user has finished their session on the PC it should be logged off (this will ensure that the next user is presented with an authentication challenge) At the end of the day PCs should be shutdown (this will save on power requirements).
- Schools should restrict software installation using group policy so that users cannot install software other than that permitted by the school. Where a user has a need for software outside the “standard build” this should be cleared with an IT person such as an ICT Coordinator so that licensing, compatibility and support requirements can be taken into account.

Backup

- Your data should be backed up on a daily basis. Your backup software should provide facilities to verify that the backup has worked - backups that have appeared to work at the time have caught out many schools, some faults (often a faulty disk) has meant the data cannot be recovered. It is good practice to regularly test your tapes and backups by performing regular data restores.
- Use of floppy disks is not good practice - their capacity is too small and they are very unreliable.
- CD-writers can be used for or DVD-writers can be used in “admin master\slave” setups. When using a file server the preferred backup solution is a tape drive.
- Backup-My-PC is the preferred backup software for backing up to CD or DVD for an “admin master\slave”
- Backup Exec is the preferred backup software for backing up a tape drive.
- For further information on backups please see **Backup Guidance for Schools v1.8.doc**⁸

Additional related areas & documents for Information

www.ictsupport.ccceducation.net

www.icttid.ccceducation.net

www.ictsecurity.ccceducation.net

www.ccn.ccceducation.net

www.ictsla.ccceducation.net

www.ictprocurement.ccceducation.net

Schools Network Security Health Check⁹

Should you need specific advice or have technical question please email:

ict.support@cambridgeshire.gov.uk

Education ICT Service Procurement Terms & Conditions apply:

In line with Education ICT Service policy of best quality, value and standardisation of schools ICT equipment, installation and configuration of admin and/or any MIS systems on other than Dell servers or PCs are charged at the full installation charge subject to the installation technician being satisfied that the equipment, including Dell equipment not supplied through the ICT Procurement Service meets the minimum standard recommended by the ICT Procurement Service.

Note: If a SIMS/Admin installation has been corrupted as part of an upgrade or support visit undertaken by non-ICT Service staff, a charge of £450 will be made to fix or if necessary reinstall the system.

⁸

http://c9s.e2bn.net/e2bn/leas/c99/schools/c9s/web/public/Techsupport_team/info/webpages/tid/Advice/Backup%20Guidance%20for%20Schools.pdf

⁹

http://c9s.e2bn.net/e2bn/leas/c99/schools/c9s/web/public/Techsupport_team/info/webpages/tid/Advice/Schools%20Network%20Security%20Health%20Check.pdf