

Data Backup

Guidance for Cambridgeshire Schools

Produced By:	Leon Cripps & Dave Ager
Reviewed By:	Leonard Veenendaal Technical Services Manager
Team:	ICT Technical Services
Date:	January 2007
Version	1.8

Table of content

Table of content.....	2
Why you should read this document	3
Summary	4
What should be backed up?	5
System State.....	5
Office and Curriculum Data.....	5
Daily Backup	7
Weekly Backup.....	7
How often should I back up my data?	7
How many tapes do I need?.....	8
Backing up on your Server	9
Verifying Backups with Veritas BackupExec	9
Frequently asked Questions.....	10
Why my backup does not fit onto a single CD?.....	10
If my backup will no longer fit onto a single CD, should I consider DVD?.....	10
How long should my backup take?.....	11
External Drive.....	11
Tape drive	11
How do I ensure my email and address book is backed up?	11
We have laptops in the school, is this data backed up?	11
Additional related Documents for Information.....	11
Managing School networks and file servers (PDF 236Kbs).....	11
Schools Network Security Health Check (PDF Kbs)	11
Manager's Checklist - Fileserver list.....	12
Manager's Checklist – Master PC list.....	12
Operator's Checklist - Fileserver list.....	13
Operator's Checklist – Master PC list.....	13

Why you should read this document

Most people regard Data Management and Backup with much the same feelings as filling in a tax form – unavoidable, unpleasant and expensive. It's certainly true that sorting out adequate backup systems in the first place is unavoidable and sometimes expensive (though the cost is usually tiny compared to the cost and inconvenience of re-inputting lost data). However, once a suitable system is in place, it is usually easy to manage and provides the school with the necessary reassurance that in the event of difficulties, the school's systems can be up and running again in a short time, probably within a day, even for quite serious problems.

Even with modern reliable equipment, computer systems will from time to time fail. In any one term, at least one fileserver or master computer will fail in one of Cambridgeshire's 255 schools, requiring the use of a backup to restore missing files or data. In addition there are numerous other occasions, for example when files get accidentally deleted, when it is necessary to resort to reinstating a lost file or document.

Schools with filesystems usually have least problems. This is because filesystems are supplied with tape drives and software to automate the process of backing up and make it as simple and reliable as possible. These systems can usually be restored completely in a short space of time because all files are being copied onto the tape.

Schools with a cheaper 'master' computer are usually at a disadvantage because the backup systems provided on these machines are cheaper due to the requirement to reduce costs. In this case, backup is usually manual rather than automatic and the media on which files are copied (usually CDs) do not have enough capacity to back up more than a proportion of files. This makes systems much more difficult to restore in the event of a major failure.

This guidance is provided as a 'hands on' guide to help schools put in place a suitable setup for a master computer or fileserver. Staff responsible for running the school's backups and managing data should use it as a handbook. Managers should use it as a guide to help them understand what ought to be done to secure the school's data and systems.

Matthew Nall
MIS Programme Manager

Leonard Veenendaal
Technical Services Manager

Summary

This document is intended for anyone who is directly involved in ensuring that the files and data held in schools computer systems are securely backed up. It aims to provide schools with information concerning recommended methods for ensuring consistency and security of data, both MIS and Curriculum, held within school. By making use of this guidance, schools can ensure that:

- In the event of a failure in the computer system, files can be restored so that at worst only one day's work will be lost
- Data is adequately protected from the loss or unauthorised access under the Data Protection Act
- In the event of fire or flood, it will be possible to recover files and data that are no more than a week old.

It is not intended to be a detailed description or configuration document for any specific backup software or hardware, more as an aid to putting together a data management strategy at school.

This document should also make you think about where exactly your users are storing their school-related data.

For example, think about laptop users who occasionally may use their laptops at home; how does their data get backed up?

Do your users store their files in "My Documents"?

Where is this folder?

Is it backed up?

If laptop and PC data is still being stored locally and not on a server, you should be seriously considering budgeting for the installation of a fileserver to centralise not only data storage, but also to centralise

- Backups
- Antivirus distribution
- User account management

We cannot stress enough the importance of all schools having a comprehensive and reliable system back up strategy. It is vital in ensuring the continued smooth running of your school systems, and should be regularly checked and validated by your own staff.

What should be backed up?

If you have a fileserver in your school servicing both Admin and Curriculum networks, you should have all of your data in one main location – on your server. Your backups should be taken care of automatically overnight onto some form of tape drive.

If you still have a peer-peer Admin network – i.e. two or more PCs sharing data between each other – you need to take extra care to ensure your data is being adequately backed up. This is because your PC does not have the same failover (fault tolerance) facilities as a file server, and is in that way a bit more likely to have complete disk failures...

You should however check to ensure the following is being backed up:

System State

On a File Server;

This backs up [Active Directory](#), where all your user accounts and file rights are held. It also backs up the registry, which holds information about installed applications, and the system volume, where your operating system is installed.

On a Peer-Peer Network (Admin Master)

This backs up the local users and groups rather than Active Directory. It also backs up the registry, which holds information about installed applications, and the system volume, where your operating system is installed.

Office and Curriculum Data

You probably have areas set aside for Office/Staff Data and Pupil Data; you should check with your system administrator if you are unsure where this area is, and also to ensure it is being regularly backed up.

The default areas setup by Education ICT Service, and used by your email clients, are in the following locations:

Location	Description	File Server/Peer-Peer
C:\schdocuments	This is the shared area on the Master PC holding all shared documents for admin Staff	Peer-Peer.
C:\documents and settings\mis Note: mis being the users login	This area holds your email plus other profile related files	Peer-Peer.
Pupil Data	Pupils work.	Peer-Peer. Due to not central storage this data could be located over a number of curriculum PC's and laptops. If you need to backup your Pupil files, contact Education ICT Service for advice.
E:\Staff\	Centralised Location for all staff data and home folders including redirected "My Documents" for laptops and PC's.	File Server.
E:\Office Share\	Centralised Location for all office data	File Server.

E:\Pupils\	Centralised Location for all pupils work	File Server.
E:\Curriculum\	Centralised Location for all planning material.	File Server.
C:\documents and settings\ <i>Username</i>	This area holds your email	File Server. Even if you have a file server you email data will still be local to your machine, in this situation you will need to seek advice from the Education ICT Service on how to ensure this data is also being backed up.

SIMS Data should be stored in the following areas:

Location	Description	File Server/Peer-Peer
C:\SimsDrv\Sims	The older dBASE files, including NOVA timetable data and FMS finance data	Peer-Peer.
C:\Program Files\Microsoft SQL Server\Data\SIMS	The new SQL data files, usually SIMS.MDF and SIMS.LDF	Peer-Peer.
C:\Docstorage\SIMS\SIMS	The Document Management Server (DMS) directories	Peer-Peer.
C:\SimsDrv\Sims\sql\sims.db C:\SimsDrv\Sims\sql\sims.log	FMS6 backup - only the SQL folder containing sims.db and sims.log	Peer-Peer.
C:\Program Files\SIMS\Dinner Money\Dindata.mdb	Dinner Money Data.	Peer-Peer. Dinner Money also has it own backup utility that should be used daily to backup to floppy or other removable media.
F:\adapps\Sims	The older dBASE files, including NOVA timetable data and FMS finance data	File Server.
F:\Program Files\Microsoft SQL Server\Data\SIMS	The new SQL data files, usually SIMS.MDF and SIMS.LDF	File Server.
F:\Docstorage\SIMS\SIMS	The Document Management Server (DMS) directories	File Server.
F:\adapps\Sims\sql\sims.db F:\adapps\Sims\sql\sims.log	FMS6 backup - only the SQL folder containing sims.db and sims.log	File Server.
F:\Dinner Money Backups	Dinner Money Data.	File Server. This is the location that is set within Dinner Money to backup to the file server rather than removable media

SQL is a newer and more efficient database format, which is used by SIMS from CP3 onwards.

These data areas should all be backed up as a group to ensure consistency of data across the databases as they are linked (particularly the SQL database and DMS). It follows that they should also be restored as a group. If for any reason you feel you should restore only a part of the system, you should seek advice from your SIMS support unit.

The SQL data files are always open as long as the database process is running. The usual solution is either to have an add-on to your backup software to deal specifically with SQL databases or to have a process

that stops the database service before the backup and re-starts the database once backup is complete and verified.

SQL Data should have been installed onto a Data area; ideally it should NOT be on the System drive, typically C:\

Again, your system administrator will be able to tell you where this is installed.

Daily Backup

Your daily backup routine should contain the following folders:

For Peer- Peer Networks:

- School Documents
- Documents and Settings for each user – contains email
- SIMS Tree
- SIMS Document Server
- SIMS Finance (FMS6)
- Capita Dinner Money

For File Server Schools:

- Where possible a full server backup should be done.

Weekly Backup

- SQL Data – from SIMS
- Daily Backup

For File Server Schools:

- Where possible a full server backup should be done.

How often should I back up my data?

Data should ideally be backed up on a daily basis. There should be a tape or backup device rotation scheme to ensure you have data going back at least 3 months, with an annual backup kept indefinitely.

How many tapes do I need?

The schedule below is the preferred rotation scheme of the Education ICT Service:

The File Server is scheduled to backup the entire contents on the hard drive every Monday-Friday night at 10.30pm.

- A suggested routine for backing up is by having 10 tapes. These are labelled and used as follows:
- Monday
- Tuesday = 4 Tapes
- Wednesday
- Thursday

- Friday 1 = 1st Friday
- Friday 2 = 2nd Friday = 3 Tapes
- Friday 3 = 3rd Friday

- Month 1 = 4th Friday of the 1st Month
- Month 2 = 4th Friday of the 2nd Month = 3 Tapes
- Month 3 = 4th Friday of the 3rd Month

Note: Additional tape to be purchased annually for yearly backup

This strategy provides you with the ability to restore data from the last week, plus any Monday over the last month, plus any month for as many monthly tapes as you have. Variations on this scheme are available, and provide a trade-off between the number of tapes required, and the number of monthly tapes available.

Backing up on your Server

A server purchased through the Education ICT Service should have been installed with Veritas BackupExec and a DDS4/Dat72, DLT 160 or LTO 2 tape drive. This provides for a complete backup of your entire server's system state, storage; operating system, applications and data files. In the event of a system failure, part or all of the system can be restored from a single tape. Files kept on individual workstations will not be backed up. Staff and pupils should therefore be discouraged from saving files elsewhere than on the network.

Backups are scheduled to run overnight when users are logged out of the system. This reduces problems with files being "open" and therefore not backed up. Special measures have to be taken with the SIMS SQL database. A number of tasks can be scheduled overnight – you will find it useful to record these with your server's operational notes to avoid clashes.

Verifying Backups with Veritas BackupExec

For added security, the Veritas software backs up the files on your server and then verifies that the files have been copied correctly. It is essential that you check that this verification has worked because if files are backed up incorrectly you will not be able to restore them – your data is at risk if this is not checked regularly, ideally daily.

- a. Press Ctrl-Alt-Delete at Server
- b. Log in as admin & enter password
- c. Click Start-Programs-Veritas BackupExec or double click Veritas BackExec icon on the desktop
- d. Ensure Job Monitor is selected at the top of the window
- e. Select Job Status tab at bottom of Window
- f. You will see in the top half of the Window that a job is scheduled for tonight's backup at either 10.30pm or 11.00pm
- g. The bottom half of the Window will report backup successes and failures.
- h. Check the date of the last backup and ensure is it for yesterday (or last Friday if it's a Monday) and that the job status reports either 'Successful' or complete with exceptions.
- i. To view brief report: Double click yesterdays Backup Job and scroll through the job report
- j. If the backup reports completed with exceptions this means that certain files have been skipped. These are often files, which need to be kept open to allow the system to continue to run. If you are not sure if your backup was successful then please call the helpline and they can check with you. Tel. 08450 450973.
- k. As part of the Education ICT Service Server Support SLA, Backups are monitored and an email alert is sent to the helpline if a backup fails, this is an excellent feature, but it does not mean that you don't need to check the backups yourself.

What else needs to be done?

- At regular intervals throughout the year you should carry out a test restore of a subset of your data. It is all very well putting tapes or CDs into your backup device each day, but the data held on here needs to be tested. Your ICT Technician should be able to help you with this, but it should suffice to take several folders or documents from the backup set and restore to a temporary location to ensure the integrity of the data. [See *Verifying Veritas BackupExec* above]
- A cleaning tape is normally provided and should be used approximately once every other week. This is done by inserting the cleaning tape into the tape drive and after period of time it automatically ejects itself.
- Tapes should be replaced on average after being used 365 times.
- Tapes should be kept in a fire-proof/flood-proof safe at all times if possible. The last night's tape should be kept offsite at all times. We also recommend that you keep the Friday tapes offsite when not being used. In the event of fire or flood these tapes can be used to restore a destroyed system. A member of staff should be designated to look after this.

Frequently asked Questions

Why my backup does not fit onto a single CD?

You are constantly increasing the amount of data stored on your PC. SIMS data is also becoming more and more complex; this is only going to increase over time.

A CD can contain about 700MB of data; in today's ICT environments this is not uncommon.

If my backup will no longer fit onto a single CD, should I consider DVD?

A standard DVD holds 4.7 GB data. If your data has outgrown a single CD then it probably would within the near future outgrow the capacity of a DVD, making it costly short term solution. A DVD+RW costs around £1.00 per disk

You also need to be careful of the number of DVD standards, these are as follows:

Note: Not all DVD writers support all standards

DVD - R is a recordable DVD format similar to CD-R and DVD+R. A DVD-R can only record data once and then the data becomes permanent on the disc. The disc can not be recorded onto a second time. There also are two additional standards for DVD-R disks: DVD-RG for general use, and DVD-RA for authoring, which is used for mastering DVD video or data and is not typically available to the general public.

DVD - RW is a re-recordable format similar to CD-RW. The data on a DVD-RW disc can be erased and recorded over numerous times without damaging the medium.

DVD + R is a recordable DVD format similar to CD-R. A DVD+R can only record data once and then the data becomes permanent on the disc. The disc can not be recorded onto a second time.

DVD + RW support random write access, which means that data can be added and removed without erasing the whole disc and starting over. This means that DVD + RWs can almost be treated like removable hard disks.

DVDs created by all of the above formats can be read by most commercial DVD-ROM drives.

DVD RAM discs can be recorded and erased repeatedly but are only compatible with devices manufactured by the companies that support the DVD-RAM format. DVD-RAM discs are typically housed in cartridges.

Recommendation

- Education ICT Service recommendation is to use DVD+RW discs.

How long should my backup take?

This really depends on how much data you have to backup and the speed of your CD-RW drive. Basically the data transfer rate of a single speed CD-RW is approximately 150 kilobytes per second. Some examples:

20x 3MB/s

24x 3.6MB/s

32x 4.8MB/s

Therefore if you have a single full CD to backup (700MB) it is likely this will take 10 minutes (Please allow time for the backup to verify).

External Drive

There are known issues and problems with the external drive being locked by Backup my PC and other backup software causing the machine to crash or only releasing it once the machine has been rebooted. Not a recommended or supported by the Education ICT Service.

Drawbacks

- One copy of your data on one single drive
- One point of failure for your backup
- If you overwrite the backup each day you have no previous backups to refer to

Tape drive

Although generally quite expensive, tape backup is a well known and reliable backup format. Generally used for Server-based backups

Drawbacks

- Expensive
- Not the quickest backup solution, although as these are normally server based, they are configured to take place overnight.

How do I ensure my email and address book is backed up?

Email and your email address book is by default stored on your local hard drive.

As long as you backup your c:\documents and settings\

For schools with a file server Education ICT Service recommend using Microsoft Outlook with a add on utility to backup email to a remote location, for further information please contact Education ICT Service.

We have laptops in the school, is this data backed up?

With more and more laptops being used by teachers in schools (often at home too) it is becoming vital to provide a backup solution here too.

The majority of newer model and indeed Education ICT Service supplied laptops are configured with a CD-Rewriter, which can be used as a backup device.

The preferred solution here is in a client-server environment where your system can be configured with “offline files”. This basically means you have a “copy” of your own data – i.e. My Documents folder – which when you reconnect to your school network will automatically be synchronised back to the server, where it will be automatically backed up overnight.

Additional related Documents for Information

Managing School networks and file servers (PDF 236Kbs)

www.icttid.ccceducation.net > Servers & Networking > [Managing School networks and file servers](#) (PDF 236Kbs)

Schools Network Security Health Check (PDF Kbs)

www.icttid.ccceducation.net > General Advice and Guidance Documents > [Schools Network Security Health Check](#) (PDF 250Kbs)

Manager's Checklist - Fileserver list

	Is the fileserver fitted with a tape drive and backup software?
	Is there an adequate backup schedule for tape changes?
	Are weekly tapes stored offsite?
	Is the member of staff responsible for backups aware of the full range of tasks (see operator's checklist)?
	Is the administrator's / backup user's ID and password stored securely for use in the system administrator's absence?
	In the event of the fileserver failing, have arrangements been made that will ensure the systems are back working in a satisfactory timescale?
	Have these arrangements been documented as part of the school's Disaster Recovery Plan and agreed by governors?

Manager's Checklist – Master PC list

	Is the master PC fitted with a backup device and appropriate backup software?
	Is there an adequate backup schedule for changes of media (CDs / DVDs / ZIP disks / etc.)?
	Are weekly media stored offsite?
	Is the member of staff responsible for backups aware of the full range of tasks (see operator's checklist)?
	Is the administrator's / backup user's ID and password stored securely for use in the system administrator's absence?
	In the event of the master PC failing, have arrangements been made that will ensure the systems are back working in a satisfactory timescale?
	Have arrangements been made to ensure that files not backed up can be reinstated (e.g. re-installation of SIMS applications, Dinner Money, Microsoft Office)?
	Have these arrangements been documented as part of the school's Disaster Recovery Plan and agreed by governors?

Operator's Checklist - Fileserver list

	Is the schedule of tape changes documented?
	Is there a system of 'checking off' tape changes?
	Are weekly tapes stored offsite?
	Is the backup software checked daily to ensure it has verified properly?
	Has a tape been tested each month?
	Are the arrangements for recovering a failed system documented?
	Is another member of staff aware of all these arrangements and can take appropriate actions in my absence?
	Is the administrator's / backup user's ID and password stored securely for use in the system administrator's absence?

Operator's Checklist – Master PC list

	Is the schedule of media (CDs / DVDs / ZIP disks / etc.) changes documented?
	Is there a system of 'checking off' media changes?
	Are weekly media stored offsite?
	Is the backup software checked termly to ensure it is backing up the right files?
	Has a backup been tested each month?
	Are the arrangements for recovering a failed system documented?
	Are all the required installation CDs / licence keys, etc. stored ready for use if needed?
	Is another member of staff aware of all these arrangements and can take appropriate actions in my absence?
	Is the administrator's / backup user's ID and password stored securely for use in the system administrator's absence?