# NETWORK WITH A SERVER

In this scenario the organisation has recently moved from having *standalone* PCs to a network and has a server installed.

The server takes the place in the example above of the shared PC. Generally the same processes will need to be carried out, but the server provides a much higher level of security as to who can access the folders. The server administrator needs to apply the permissions – training is necessary for someone new to server admin.

The staff team still needs to decide who has access to which folders. This is, of course, not set in stone, staff can be added and removed as necessary but it helps to have some sort of plan. For example, the finance worker and the director probably both need access to the Finance folder, but only the director to the Personnel files. If there's a management team then they can share certain folders that only they need access to and so on.

Remember that it is not just a question of confidentiality, but also of security – if an inexperienced user wanders into an area where they shouldn't be and accidentally deletes files it could be problematic. Security protects you against this as much as it does against malicious hackers - who in reality are much less likely to be wandering around your network. Folder names are visible to anyone with access to the server but they won't be able to open or save documents to the folder

unless they have the relevant permissions. Folders or sub folders can be made *read only* to certain users so that changes to documents cannot be made – you may want staff to be able to see the staff handbook information but not be able to alter it.

It is good practice to set up a few virtual drives (see drive mapping above) – your network contractor who's setting up the sever can do this for you. On a server you might have three mapped folders - letters allocated here are arbitrary:

- G: Company – where the organisation stores all its work files (finance, personnel, projects etc.)
- S: Shared – templates, forms, resources, staff handbook, temporary files such as Antivirus updates etc.
- U: Users – personal documents (each staff user has their own specific folder which can only be seen by them)

## Hints and tips

Agree on *naming conventions* for files and **be consistent** in using that convention. If you have a "Board meetings" folder and a sub folder called "Minutes" and under that "2003" there's not much point in naming a file "Board meeting minutes 3 July 2003" when something more abbreviated would do. However, ensure that files that are misfiled (it happens!) can be identified relatively easily.

Avoid using “miscellaneous” folders – they will just end up with all sorts of odd stuff that needs sorting out later. Instead, try to file everything appropriately – if it doesn’t fit into a folder then perhaps the folder you want is missing so create a new one (you might need some sort of system to request new folders so that things don’t get out of hand).

Another thing to avoid is using the term New in filenames - a time will always come when a newer version of the file comes along, and having New2, New3 etc isn't very helpful.  Do mark final versions of a file as Final however - and stick to it!  If a more final version of the file becomes available rename the old one so it doesn't say final - if someone finds a file marked final they will not look for one marked final 2!

There is nothing worse than opening folders which are empty and finding all the files you would expect to find in them in a long list below them. Think of it in terms of your filing cabinets – you’d not be happy if everybody just chucked their papers in the bottom of the filing cabinet drawer without filing it in a folder – how would you find it again?

Make sure existing staff are given training in the new file management systems and that new staff receive induction so that they know where to find and file documents. It may well be worth producing a short manual to assist staff, or

creating a page on the company intranet if you have one.  Set out clearly your conventions and who is allowed to make new folders, when and where.

Your ICT Induction Manual (see the knowledgebase article ICT Induction Manual) may also need to contain guidelines on user responsibilities with regard to file management. Check on legal requirements for how long electronic documents, including emails, must be stored.

**Back up your data!**

This cannot be stressed enough – the best folder structures in the world aren't worth much if the hard drive fails and you don't have a recent back up. Make a back up policy and stick to it.

Source: http://www.ictknowledgebase.org.uk/directorystructures