## Security measures to be used when storing data

The storage of data is one of the most important areas in any business organisation regardless of the size of the business. Lack of security can mean the hacking of data by competitors, people with a grudge against the company, fraudsters, blackmailers or, indeed, anyone who thinks they could have something to gain by disrupting, destroying or stealing the information.

### Network/computer security

#### Usernames/passwords

A username is not necessarily a unique name that allows a user to gain access to a particular area on a network. A password is also required and this is a unique code that enables the user to log on to their individual files within this certain file or area on a computer system. The network system administrator sets the username. They decide what the user desktop should contain in terms of application software and what security they want to apply to this area. The username is then given to a group of people. These people can access this group of files but to keep their work in this area individual they also have to use a password which has to be set uniquely by each individual user to the system.

Password and user files are both stored on the computer system. When the user enters the password and/or username this is compared to a list of passwords/usernames stored on the computer system. If a match is found, the user is allowed to enter the designated area.

#### Access rights/permissions

Every document/file on a network can be set to have certain access rights and permissions. These tend to be read-only or read/write and are set by the network administrator. This means access can be restricted to certain groups and thus assists with security issues. For example, in a business context, a salesperson does not need to access payroll files and wages and payroll personnel do not need to access the sales figures.

Levels of access can also be set in which different people are granted access to different levels of permissions. For example, in a classroom a junior pupil might be completely restricted to what they see on the screen in front of them, whereas a more senior pupil not only can gain access to a screen, they might also be allowed to change the size of the icons or the background for themselves.

### Document security

With the advent of remote computing document security is even more important. Some security you can set yourself through the file or through special document security software.

The main method of document security is through the use of passwords but there are others which are indicated below.

#### Passwords

Passwords can also be set within the software as well.

This tends to be set by the user of the document and it is their responsibility to administer this password.

Features of a good password

Users need to be careful that others do not get access to their password and, therefore, they need to make sure it is:

 not easy to guess

 long – at least eight characters

 a combination of letters and numbers

 not written down where others would find it

 changed regularly

 not a word found in a dictionary

 not shared with anyone else

 unique to the area they are using

#### Other ways to restrict access to or editing of content

 Restrict email permission, e.g. block the sending of attachments

 Use a business watermark on documents which will deter people from passed the documents on

 Set permissions on the document, e.g. a print request automatically generates an email to the correct person who will either decline or accept this request

 Give a document a level of protection if it is being shared, e.g. lock down a document if it is sent outside an organisation

 Set a document expiration time – time bomb

 Use software which does not allow editing such as PDF software

 Use software which can wipe out documents when necessary

 Track access on mobile documents in terms of locations and user identity

 Encrypt any data sent

 Lock files as read-only, etc.

 Install software that alerts to any updates being carried out

 Use good anti-malware tools