JOHN OSBORN
EXEMPLAR

UNIT 1: ICT SKILLS FOR BUSINESS

TASK 1: Safe working practices in a business environment.

ASSESSMENT CHECK LIST

TASK	Student	Teacher
PASS: Describe the potential danger and at least one measure to protect personal health in an office environment.	JO	
PASS: Describe the potential dangers and at least one measure to protect physical safety in an office environment.	JO	
PASS: Describe the potential dangers and at least one measure to protect your files from loss in an office environment.	JO	
PASS: Describe the potential dangers and at least one measure to protect files from unauthorised access in an office environment.	JO	
MERIT: Describe the potential dangers and an at least two measures to protect personal health in an office environment.	JO	
MERIT: Describe the potential dangers and at least two measures to protect physical safety in an office environment.	JO	
MERIT: Describe the potential dangers and at least two measures to protect your files from loss in an office environment.	JO	
MERIT: Describe the potential danger and at least one measure to protect your files from modification in an office environment.	JO	
DISTINCTION: Describe the potential danger and at least two measures to protect your files from modification in an office environment.	JO	
DISTINCTION: Describe the best way to go about choosing a strong password.	JO	

OVERALL GRADE FOR AO1 - DISTINCTION

Press *Ctrl + Home* to return to Assessment Check List

OCR National Level 2 (ICT)

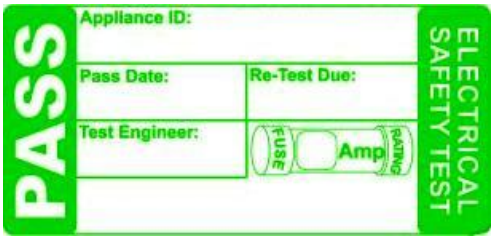
1. ***Protecting health in an office environment*** *(P)* *(M)*

Comment [p1]: Well done on this task you are heading for a distinction! JO

Personal health whilst using ICT equipment in an office environment of the upmost importance. Should an employee suffer health problems due to improper use of ICT equipment then it could result in lost productivity and potential legal claims. There are a number of issues that may affect employee health and there are measures that can be put in place to prevent any problems. Posture is of great importance when using a computer to help prevent back problems. To prevent this, computer users should ensure that they have a fully adjustable chair that supports the back, suitable footrest and a screen that can be tilted to a position that prevents them having to be in a painful position. The first picture above shows bad posture and the second picture shows good posture. People who do a lot of typing could suffer from repetitive strain injury or RSI. This is where damage occurs to the fingers, wrist and other parts of the body due to repeated movements over a long period of time. When looking at a computer screen for a long time it is possible to suffer from eye strain .This can be prevented by using screen filters, taking regular breaks and ensuring that the work area has suitable lighting with minimal glare.

Press *Ctrl + Home* to return to Assessment Check List

2. Protecting physical safety in an office environment (P) (M)



An office is potentially dangerous place where there can be a number of threats to physical safety when using ICT equipment. Trailing wires in an office could be a tripping hazard and should be avoided using cable management systems or running wires in trunking. A common problem in offices is the consumption of food and drink close to electrical equipment. If fluids get spilt into computers or other ICT equipment it can cause great damage with possible risk of electrocution. Training and signage (see picture) should inform office workers not to eat or drink near computers. It is also a good idea to ensure that all electrical equipment in an office is PAT tested on a regular basis to ensure it complies with safety standards. A typical PAT testing label is shown above. otential dangers and the measures you would take to protect health in an office environment

Press *Ctrl + Home* to return to Assessment Check List

3. Protecting files from loss in an office environment (P) (M)

Data in an office environment is often of great value and measures need to be taken to ensure that it is protected. Files can be lost because of accidental deletion, virus infection or a physical disaster (e.g. a fire). Backups provide a good way of ensuring that data is not lost by having a second copy stored somewhere else, for example on a server back up tape (see picture above)or USB stick. Important files should not be stored on local machines and must instead be stored on network locations where they can be backed up. It is also important to ensure that files are stored in sensible folders structures which are clearly named. Sometimes with very important data backup mediums (tapes, DVD's, Server Clusters) should be stored in a physically separate location.

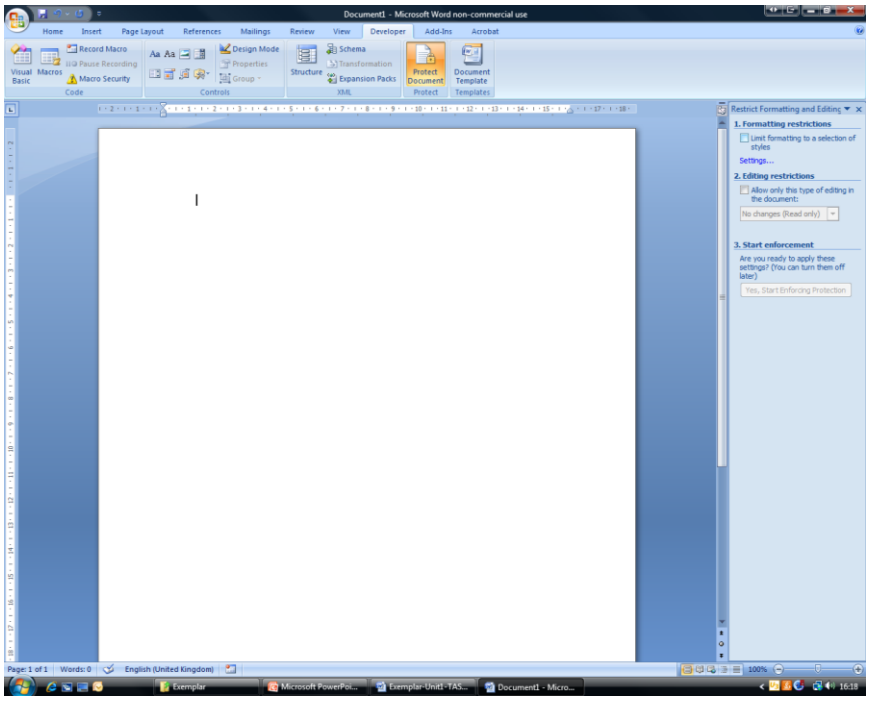
Press *Ctrl + Home* to return to Assessment Check List

4. Protecting files from unauthorised access in an office environment (P)

The best way to protect files from unauthorised access is to ensure that you have a strong password that you do not share with anyone else. It is also important not to leave your computer whilst you are still logged on. If you don't want to log off you should lock the machine. Some virus attacks can allow unauthorised access to your computer so it is important to ensure that you have anti virus software installed and that it is up to date.

Press *Ctrl + Home* to return to Assessment Check List

5. Protecting files from modification in an office environment *(M) (D)*



Files can be protected from unauthorised modification by using password controls. Within a document you should make sure that passwords are set that only allow certain types of access. Eg. Read Only, Modify etc. Any passwords that are set should be strong and not shared with anyone else. The screen shot above shows Microsoft Word's password control which can be found under the Developer tab. In addition it is important not to allow anyone to use your computer whilst you are logged on.

Press *Ctrl + Home* to return to Assessment Check List

***6. Guidance on choosing a strong password** (D)*

Strong passwords should never be based on dictionary words and should contain a mix of upper and lower case letters along with some numbers and some special characters (%,&,*," etc.) The password should not be too short (at least 8 characters) and should not be associated with anything that could be easily guessed (e.g. car number plate)

Press *Ctrl + Home* to return to Assessment Check List