Using portable storage devices safely

Portable storage devices are devices that connect to the USB port of a computer and are used to store and retrieve data. Examples include:

- USB sticks/thumb drives
- iPods
- PDAs
- smartphones
- digital cameras
- external hard drives.

A portable storage device such as a memory stick can be a very useful item to have. However, there are a number of security issues surrounding them:

- they can carry viruses bypassing the many security measures put in place that would normally stop viruses spreading
- confidential data stored on devices could be divulged if the storage device becomes lost or stolen
- data could be corrupted if the storage device is not properly removed from the computer.

If you are storing irreplaceable data on a storage device we recommend you keep a copy of it on a network drive. Network drives are backed up daily.

You do not have to use a storage device to move files from one computer to another. If you are moving from one computer to another on our network, it is better and safer to email the file to your Outlook account. When you get to the computer the file needs to be on, log in to your Outlook account and access it there.

Minimise the risks

Viruses

When you connect a portable storage device to a council computer we recommend that you run the Sophos anti-virus product. This will make sure that the storage device has no virus on it.

This does not happen automatically for performance reasons.

To scan a portable device:

1. Click the start menu at the bottom left of the screen.
2. Select "Computer".
3. Right click on the drive.
4. Select the option "Scan with Sophos Anti-Virus".

5. The scan may take a few seconds or even minutes depending on the amount of data stored do not try to access the data on the storage device until the scan is complete.

Data

You should only transfer data to the device which you are authorised to share with others inside or outside of the council.

Personal portable storage device

You can use your own, personal portable storage device if authorised by your line manager.

If you are authorised to use your own storage device you must:

- follow all the rules as stated in this guide
- not keep any sensitive or confidential information on the storage device unless it is encrypted.

Encryption

Any portable storage device connected to a Council owned Windows 7 computer will be encrypted (disk and its contents) if any files are saved to it.

If you want to avoid your personal device being encrypted you should only attach council supplied storage devices to council-owned Windows 7 compters.

Once a storage device is encrypted you can read and write to it using a computer running one of the following:

- Windows 2000
- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 10

If you wants to remove encryption from a device, this can only be done once the device has been unlocked using a password. Alternatively the device will have to be re-formatted.

This measure is being taken to protect the council's information if the device was lost or stolen. The council will not be held liable for any portable storage device becoming encrypted after it is connected to the council's network.

Safely removing portable devices

Before removing a portable storage device you must make sure that it is safe to do so. If data is still being transferred between your computer and the storage device when you take it out, it is likely that the data will be corrupted.

To remove the storage device safely:

1. Click on the safely remove hardware icon (a picture of a USB device with a tick in a green circle) in the task bar at the bottom right-hand side of your screen.
2. In the menu that appears, click once to eject the relevant device.
3. A pop-up bubble will appear in the bottom right-hand side of the task bar informing you it is: "Safe to Remove Hardware".
4. Unplug your storage device