## Connecting peripherals to computer devices

All peripherals, e.g. printers, digital cameras, mice or external devices, require connection to computer systems. They can be connected using wires or wirelessly.



### Wired methods

Peripherals that use wires tend to be connected through one of the ports available on the computer system.

USB devices include pen drives and Internet dongles. The receiving computer needs appropriate driver software on the system to enable recognition of the plugged-in device.

Another method of connection is called Firewire. Firewire permits up to 63 devices to connect to its bus. It allows information to be quickly transferred between digital devices, such as digital cameras, home entertainment centres, printers and scanners, and computer systems. In modern terms it is classed as a plug-and-play device,as when you plug the device in to the port, the operation system automatically detects it, applies the appropriate driver software if present and, if not, asks for the software source. Its long-distance capability allows equipment to be placed in businesses at appropriate locations.

### Wireless methods

#### Wi-Fi

Wireless Fidelity (Wi-Fi) is used to connect computers or other hardware together that come within range of each other. Each device requires a wireless adapter. Other computers can join the network provided they are within range. A hotspot is required – a site that offers Internet access by using a router connected to an ISP. The user opts to connect wirelessly and inputs a password to connect to the ISP. This hotspot or AP (access point) can also act as a connector between a wired network and a non-wired network.

#### Bluetooth

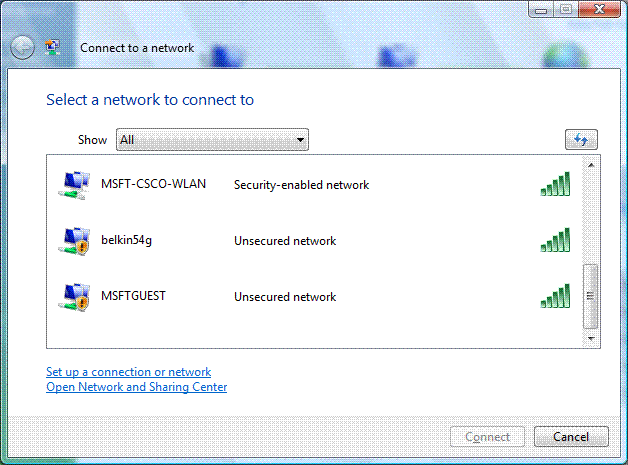
****Bluetooth is another wireless technology that allows devices such as phones, etc. to communicate over short distances. Bluetooth may already be installed in a device and thus a driver is not required. The idea is to pair one device to another using a passcode which is exchanged between the two devices. The first device asks for the password the user invents and then the second device asks for it. When the password is given correctly the two devices can communicate. Bluetooth is very popular for sending photos to your phone, sending voice from a headset to a mobile phone or backing up PDA data to a mobile phone.

#### Infrared

Connecting peripherals using infrared requires infrared adapters. This is usually an external device connected to a PC computer system and an internal device in, for example, a mobile phone. Although it has the advantage of not needing cables, the two devices trying to connect must be in direct line of sight. Businesses usually use infrared for computer mice and printers. Infrared is also used for night vision and hyperspectral imaging such as that used in security systems.

## Connecting a computing device to a wireless network

Apart from requiring the appropriate technology and software on the devices you are trying to connect, mostly for security reasons, there are some other features required for the connection to be successful. The following are some examples:



### Network name (SSID)

An SSID (service set identifier) is the name of a wireless local area network (WLAN). All wireless devices wishing to connect must use the same SSID in order to communicate with each other.

If a network is hidden then an SSID can be entered manually. It is also possible for a public SSID to be broadcast from an access point to all wireless devices that are within range of each other.

### Security keys

Security keys are used to exchange messages between devices. These are commonly encrypted with WEP (Wired Equivalent Privacy). This is set through the network router setup wizard. It is a sequence of hex digits chosen by a network administrator and assists with securing the network connection. As with all technology WEP has been superseded by WPA(Wi-Fi Protected Access) and WPA2 which provide greater security.

### Firewall settings for public and private networks

#### Public

The firewall setting is applied when a connection to a domain is made through a public network, e.g. hotel airport, coffee shop. A network profile is dynamic – it recognises how the computer connects to the network and changes automatically. The actual security is controlled through the operating system. It is applied to a network adapter when applied to a public network. The user sets the profile.

#### Private

The firewall setting is applied to a network adapter when it is connected to a network that is identified by the user or administrator as a private network. A private network setting is one not directly connected to the Internet but is behind some kind of security device such as a NAT router or hardware firewall. It is set through the operating system.