Wireless and Wired Networks

	Wired network	**Wireless network**
Advantages	• Connection speeds are typically faster • Typically have higher bandwidth • Typically have better security/fewer security risks	• Typically lower setup costs • No wires/cables are required • It is easy to connect new devices • Users not confined to a single location // Users can connect to the network as long as they are within range • Can connect multiple devices without the need for extra hardware
Disadvantages	• Cables can be hazardous and unsightly • Not all devices can connect via cable eg some tablets • Can be expensive to set up	• Connection speeds can be slower • Connection speeds can reduce the further from the WAP you are • Subject to interference from walls, objects and other nearby electronic devices • Typically less secure • Connections are not as stable as wired networks
Security issues	• Typically more secure than wireless as need physical access to the network to intercept data	• Risk of theft of bandwidth by neighbouring users within range • Risk of data loss/data being stolen unless encryption is used • Typically easier to intercept data/'hack' network // Wireless transmissions can be intercepted by anyone within range of the router

EEL points for anyone allowing wireless access:

- Websites – need to restrict access to inappropriate websites
- Time – limit amount of time, they may not want to provide indefinite access or may want to charge for access after the time limit has expired.
- Preventing file sharing and illegal sharing\use of copyrighted materials.
- Accountability – identification of users and actions on a network by preventing anonymous access.
- Prevention of illegal activities such as terrorism and fraud.
- The responsibility to keep children safe and protected.
- Responsibility to keep users (customers) data safe and secure. Risk that data may be recorded and used for marketing etc…
- Spoofing of websites, phishing. Responsibility of organisation to put some kind of protection in place, eg filtering of known fraudulent sites. Risk of malware or other risk to hardware
- Recording of private messages or details if not encrypted.
- Recording of usernames and passwords that the user may also use to access other systems.
- Responsibility of organisation to secure their systems from possible attack.