

Unit **01**

Fundamentals of IT

ABOUT THIS UNIT

In order to create, manage or develop information technology systems, you need to understand how the components and software work and their individual purposes. However, these components must be able to communicate with each other to carry out tasks as varied as calculating the price of your new tablet, monitoring medical implants and navigating spacecrafts to the very edge of the galaxy.

This unit will help you to develop your understanding and prepare you for the units to come. However, you will understand more if you are able to study examples of real systems, hardware and software and so, if the opportunity arises to study this unit alongside the more practical units, through work placement or study of systems that you already work with, then take it.

This is a mandatory unit for this qualification.

LEARNING OUTCOMES

The topics and activities in this unit will help you to:

- 1 Understand computer hardware.
- 2 Understand computer software.
- 3 Understand business IT systems.
- 4 Understand employability and communication skills used in an IT environment.
- 5 Understand ethical and operational issues and threats to computer systems.

How will I be assessed?

You will be assessed through an external assessment set and marked by OCR.

LO1 Understand computer hardware

GETTING STARTED

(10 minutes)

In pairs, produce a list of computer items which you consider to be hardware and display it for everyone to consider.

1.1 Computer hardware

How do you recognise hardware? It is anything in a computer or information system which you can touch – but remember it is unwise to touch any components that are live (carrying an electric current). Another way of remembering how to identify hardware is that if you drop it, it will be damaged or broken.

The range of computer hardware increases all the time, as **computer components** become smaller and more powerful. Some examples are listed below; take the opportunity to investigate others, especially their uses, benefits and limitations.

Input devices

A computer is only useful if it can communicate with its external environment. **Input devices** enable the user to communicate with the computer and **output devices** allow the computer to communicate with the user.

Keyboard

The keyboard is still one of the most common methods of inputting data or instructions to a computer. The keys allow access to a range of alphanumeric characters, special characters such as '/' or '€' and a number of commands by using the function keys. It also provides shortcuts to specific tasks, for example by pressing the keys Ctrl/Alt/Delete together, the task manager box appears on the screen.

It is not always possible or appropriate to enter data using a keyboard and so other devices are available.

Mouse

A point and click device, the mouse allows the user to communicate with the computer by placing a cursor at a particular point on the screen. The computer screen tracks the movement of the mouse and normally displays its location on the screen as a cursor.



▲ **Figure 1.1** The inside of an optical mouse

KEY TERMS

Computer components – items which together form a computer system.

Input devices – devices that allow the user, which may be another computer or a measuring device, to give instruction or provide data to the computer system.

Output devices – devices that enable the computer system to provide information, data or instructions to another user, which may be computer or human.

Scanner

This input device converts a document or photograph into a digital file that a computer can read or display. Scanners have been developed for other uses such as biometrics. Examples include iris and fingerprint scanning, where the iris or fingerprint is illuminated and photographed.

Sensors

Sensors are physical devices such as thermometers, motion sensors and microphones that send signals to the computer. These signals enable the computer to decide whether an action must be triggered. For example, if a burglar alarm is set, any signal received from the motion sensor suggests that someone is in the building and the computer triggers the alarm.

Microphone

These record instructions from the user, or other sounds that the user wishes to collect. For those who cannot use a traditional keyboard or mouse, this is a very useful device for inputting data.

Graphics tablet

This can be used in a similar way to the keyboard by tapping on **icons**. It is also useful for entering data, such as handwriting or drawings of objects which cannot be captured easily in other ways. It can be hard to control if the sensitivity is set too high or too low, although this can often be adjusted via the software.

**KEY TERM**

Icon – a symbol or image on a computer screen of a program, option or selection.

Visual display unit (VDU) or screen

This is predominantly an output device, because it displays requests or information from the computer. It does, however, aid the user who is inputting data or instructions because it allows the user to check their work visually, allowing them time to correct errors before confirming their decision.

Barcode reader

This device may be handheld or static, and is used to capture information from a barcode by using a light source, scanner and decoder. They reduce the errors often introduced by manual input. In your coursework, this is recoverable as it can be pointed out and corrected but if, for example, you were dispensing powerful drugs, a wrong letter or digit could have serious consequences.

GROUP ACTIVITY**(30 minutes)**

In small groups, research three input devices and produce a brief presentation for others in the wider group explaining the technology of each one, their advantages and disadvantages.

Input and output devices

The touch screen is an example of a single device that can both receive and display data and information. The technologies used to enable the position of a finger or pointer on the screen include: infrared (IR), capacitive and resistive touch.

Table 1.1 Touch screen technologies

Type of touch screen	Explanation
Infrared (IR)	Uses IR emitters that send out infrared light which travels through the glass of the screen. On the other side of the screen is an IR receiver that collects the IR light. If the screen is touched, some of the light is scattered and the receiver records the less intense light. Complex mathematical equations calculate the location of the touch.
Resistive	Uses a glass panel covered by a thin flexible film. Both are covered in a thin metallic coating that has a small electric charge. There is a narrow gap between the glass and the film. When the screen is touched the two metallic coatings make contact, resulting in a change in the electrical charge. This change identifies the touch point.
Capacitive	Uses a glass panel with a clear electrode layer on top covered by a protective layer. When a finger touches the screen, some of the screen's electrical charge transfers from the screen to the finger as it reacts to the body's capacity to store electrical charge. This reduction is detected by sensors at the four corners of the screen, which enable the touch point to be identified.

Output devices

These allow the computer to communicate with the user.

Visual display unit (VDU) or screen

See previous page.

GROUP ACTIVITY

(60 minutes)

In small groups, research the different types of computer screens available and produce a short report on the following features:

- method of display
- resolution
- picture quality
- screen size
- the effect of price on quality.

Printers

There are different types and sizes of printer but the purpose of each is basically the same – to produce hard copy of documents, data, information, images and photographs. Types of printer include inkjet, laser, photo printers, LCD and LED, line printers, thermal printers and 3D printers.

GROUP ACTIVITY

(30 minutes)

Research different types of printer. Each group should explain how each printer works and compare: quality of type speed, impact or non-impact printers, font and graphics and main function.

As a whole group, discuss how these characteristics are influenced by price, and how they affect the usefulness of the product, together with benefits and limitations.

Plotters

These are machines used in areas such as computer-aided design (CAD) for large and accurate drawings from architectural designs to the latest space probe. Originally plotters used a pen to draw lines on paper, and later multiple pens brought colour into the process. While pens have been almost completely replaced by inkjet and laser print systems, it does help us to understand the process to remember that plotters are based on pens. The two main types are the flatbed and drum plotters.

Imagine that your arm is the pen holder, you have a pen in your hand and there is a large piece of paper on the table in front of you the size of a flipchart page. Follow these commands:

- 1 Raise your pen off the paper.
- 2 Move it to the bottom left-hand corner.
- 3 Move vertically 10 cm.
- 4 Move horizontally 15 cm to the right (point a).
- 5 Place pen nib on the paper.
- 6 Move pen 20 cm to the right (point b).
- 7 Move the pen 30 cm vertically (point c).
- 8 Move the pen to point a.
- 9 Raise pen off the paper.

Well done – you have just drawn a right-angled triangle using a flatbed plotter named 'You'!

Developments in technology mean that most pen plotters have been replaced by inkjet and laser heads which move across the paper faster and provide better quality prints.

Speakers and headphones

These provide the user with audio output. The speakers convert the electronic signals in the sound card to sound waves that can be heard by the user. Speakers broadcast to everyone within earshot, which can be a problem if confidential matters are being discussed. Headphones ensure that privacy is maintained; however, the volume of the output can result in temporary or permanent hearing loss if it set too high for any period of time.

Braille terminal

This is a specialist reader for visually impaired users. It displays text through individual cells on the terminal, each of which has rounded metal or plastic pins that protrude above the surface of the cell. The user reads the text or instructions by interpreting the pattern of the pins, just as they would if reading a book written in braille. As the user moves through the text so the braille cells update to form each word. The number of cells can vary between 12 and 84, but for non-portable terminals it is usually 40 cells.

Communication devices

These devices allow one computer device to communicate with another. Some examples are briefly explained in Table 1.1 and more technical detail is given in LO1.5.

When designing apps, consider the needs of visually impaired users. The app should allow for the ability to increase font size and change text and background colours to enable those with some sight to read the app. Ensure that the content is compatible with screen readers so that the content can be heard rather than read.

Table 1.2 Types of communication device

Device	Purpose
Modem (MOdulator-DEModulator)	Although now outdated, modems were one of the first technologies to enable computers to communicate via a telephone line. The modem converts digital signals produced by the computer into an analogue signal, which is required by the telephone line, and another modem converts the signal back to digital format at the other end so that the receiving computer can understand the message. A modem can convert both an outgoing signal and an incoming signal.
Network interface card (NIC)	A card that enables computers to communicate with other computers in a network. It is the hardware connection between the computer and the network cable.
Terminal adapter	Allows the computer to link into an Integrated Services Digital Network (ISDN).
Wireless router	Converts an internet signal into a wireless signal, which the computers and other devices in the network can use to communicate with each other and the router.
Wireless network cards	The means by which the computer and other devices are able to receive and send wireless communication.
Hub	Allows multiple computers to communicate over a network. A USB hub allows multiple peripherals to connect through a single USB port.

GROUP ACTIVITY**(20 minutes)**

Identify three uses, three benefits and three limitations for each of the devices identified above or during group discussions. These should be considered by the whole group to reach an agreed view.

1.2 Computer components

Processors (central processing unit (CPU))

The **CPU** (also called processor or microchip) manages all the hardware activities required to receive instructions and data, actions them using the input data and outputs the results. It also manages the various storage devices, both internal and external to the computer, and records where all programs and instructions are located for future retrieval.

The first CPUs had a single core, so they could only carry out one instruction at a time. The next stage was the ability to begin a second instruction before the first was completed, taking advantage of the time that the CPU was waiting for a request or instruction to be completed by the hardware under its control or the human user. Now multicore processors have two or more independent cores integrated on a single chip multiprocessor or linked together in a package. These developments have resulted in a computer being able to run multiple packages.

**KEY TERM****Central processing unit (CPU)**

– the unit that controls the actions of the computer system and manipulates the data required for particular tasks.

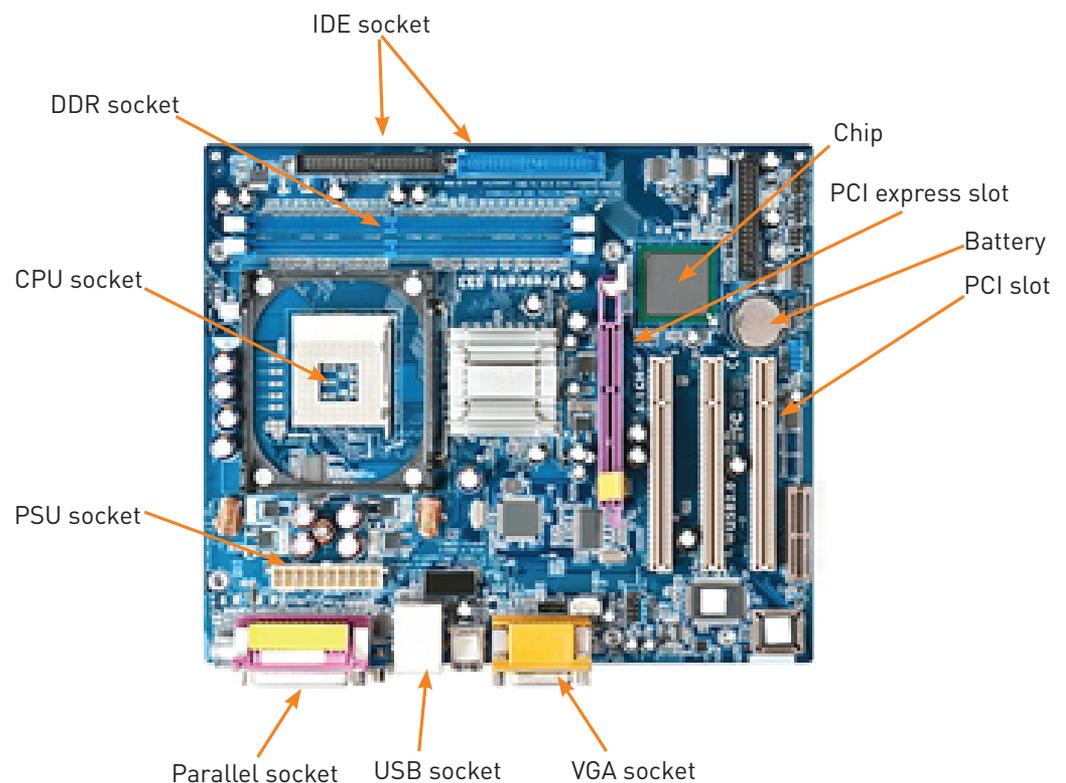
Table 1.3 The components of the CPU

Component	Purpose
Control unit	Ensures that the instructions required to operate the computer are retrieved and interpreted in the correct sequence. This means that instructions and data are transferred from the input or storage devices and placed in the temporary storage of registers in the CPU until the necessary data is ready to be processed in the arithmetic logic unit (ALU) and results stored in the right place.
ALU	Here the computer undertakes the mathematical or logical operations required to complete the instruction. The data is placed in a special register called the accumulator and arithmetic (additions and subtractions) and logical operations such as 'and', 'or' and 'not' are carried out.

Each motherboard is designed for a specific CPU and, as CPU types are not interchangeable, you must ensure that, when purchasing your new motherboard, it is designed for your CPU.

Motherboard

This is the main printed circuit of a personal computer. Components such as the CPU are directly connected to it via sockets; others such as hard drives or network cards use expansion slots or ports. Its printed circuits form the data or communications highway for the computer, ensuring that data and instructions can be transferred or stored where they are needed and located when required.



▲ **Figure 1.2** Typical features of a motherboard. Note that actual components vary according to the age of the motherboard

Computer storage

A simple way of thinking of how data and instructions are stored in a computer is to split them into two different categories: primary storage and secondary storage.

Table 1.4 Primary storage

Primary storage device	Purpose
Registers	This is small, fast and is used chiefly by the CPU to store: <ul style="list-style-type: none"> • data which is to be processed within the ALU • the instructions that inform the CPU as to what is to happen to the data • a third type of information which is that of the operating system which oversees the basic tasks required by a particular computer. (Operating systems are further discussed in Section 2.4.)
Random Access Memory (RAM)	Fast, but slower than those within the CPU and larger in size. It holds almost all other data and instructions that the computer may need for any programs open on the computer. As the programs' requirements change or programs are replaced by others, so the memory is overwritten with the new data and instructions.
Read Only Memory (ROM)	This contains permanent instructions such as the Basic Input/Output (BIOS) program, which, when you switch on the computer, checks that all the expected devices are in place, checks that they are working and loads the operating system into the computer. The BIOS is an integral part of the computer when it is built, unlike operating systems, which can be added later.

Types of primary and secondary storage can be described based upon their location or the protocols they use. One of the most widely used is the Serial Attached SCSI (SAS) protocol that follows the same protocol as SCSI but transmits data serially, one bit at a time along a single wire. These devices can handle up to 3.3 gigabits of data per second and up to 128 devices.

Storage can be internal (held within the machine) or external (where a separate device is attached to the computer through a port). These external devices can be portable – they can be moved from computer to computer and place to place.

GROUP ACTIVITY



(30 minutes)

In small groups, research the following types of external storage devices, with their strengths and weaknesses, and record your findings in Table 1.5. Copy the table onto a piece of paper if you need more space to write. Discuss your findings with the other groups.

Table 1.5 Types of storage

Storage device	What is it?	Strengths	Weaknesses
Flash drives			
Cloud storage			
Solid state discs			
Optical hard drives			

Discuss the disadvantages of each storage device identified in the table and explain what can be done to reduce their effect.

.....

Computer ports

A port identifies the location where a communication channel enters or leaves the computer system, for example on your computer you may see the USB, fire wire, mouse and keyboard ports. It is the point at which a device is plugged into the computer and normally has an interface which converts data into the correct format. Each port has a number that allows the computer to identify and select a particular peripheral easily. The different types of port can be identified by their external shape.

Table 1.6 shows some different ports available on a computer.

Table 1.6 Types of port

Device	Explanation
Universal Serial Bus (USB) port	USB ports enable the computer to connect with standalone devices such as printers, cameras, camcorders, broadband modems and mobile devices. The term Universal Serial Bus refers to the standard for digital data communications over short distances covering the cables, connectors and communications protocol used by these devices.
Fire wire	Similar to USB in architecture, but conforms to the IEEE 1394 standard so allows different elements to communicate without being linked through a computer network (peer-to-peer). This type of port often links devices which need high speed transfer of large amounts of data (such as camcorders and DVD players) to computers using special cables but, as long as the devices conform to the standard, any computer or peripheral can be linked together.
Serial Advanced Technology Attachment (SATA)	This allows devices such as optical and other hard drives to link to a computer. The port is linked to another port on the motherboard with a 7-pin ribbon cable.
Network ports	The physical ports are those which connect computers to modems, routers or local area networks.
Ethernet port	Used for cable-based networks. Most computers have at least one such port which is linked directly to the computer's network card.

The connection between devices on a network is called a channel, of which there are several types.

A channel can be optical fibre, coaxial copper or twisted pair cable carrying data between storage devices or between a computer and a storage device at high speeds of up to 10 Gbps.

Expansion cards are printed circuit boards, much smaller than the motherboard, which have a connector which allows them to be inserted into an expansion slot on a motherboard.

GROUP ACTIVITY

(30 minutes)

In small groups, investigate the following expansion card types and produce notes on the examples you find, including how each supports the computer in carrying out particular activities. Share your findings with the wider group.

- 1 sound cards
- 2 graphics cards
- 3 storage controllers.

BEWARE! Power supply units should only be opened by an experienced technician when the mains power has been disconnected. Some power supply units can hold a potentially lethal charge for weeks.

Power supply units (PSU)

The power supply unit receives electricity from the mains (alternating current or AC) and converts this into a form which the computer can use (direct current or DC). All units need a cooling system, which in PCs and servers is usually a fan system. Very large computers may use water coolant systems.

1.3 Types of computer system

There are various different types of computer system and we consider a small range here. You should research these and other examples you may discover, considering where they are used, their benefits and limitations and also justify the suitability of each system in a given context.

Desktop systems/servers

The computer can be either made up of:

- individual components, such as screen, keyboard and mouse, with a case which contains the motherboard, CPU, power supply, hard drives, optical drives and connectors and expansion cards
- a single screen and case which incorporates the motherboard and everything else. These all-in-one PCs reduce the space required to house the computer and the need for so many cables. They are also more easily moved. However, the ability to upgrade or repair the hardware is limited compared with the traditional desktop: they are also costlier than traditional desktops.

Desktops allow the user to carry out a range of activities, including document creation, data manipulation, game playing, design and communication facilities for personal or business purposes.

Tablet/hybrid

A laptop or tablet can be used in a variety of locations. The components found in an all-in-one PC are found in a laptop or tablet, but in the case of the laptop the mouse function is replaced by a touch pad and keyboard combined. Many modern laptops can fold back, effectively turning them into a tablet with a screen-based virtual keyboard. They can perform many of the functions of the traditional PC, but the screen size can be restrictive, especially if several documents need to be open at the same time. Loss or theft is also easier.

Smartphones

Smartphones can run applications, send and receive emails, take photographs and videos, record sound, act as a GPS system and run apps to provide entertainment via your record library, your e-book library and your latest game. You can create documents, manipulate data or set your alarm. However, they can hinder human interaction, and reduce spatial awareness when being used.

Security is another issue, as an unlocked phone left in public allows anyone who finds it access to your private life, username and password for your cloud storage if you don't log out of apps properly. The malware and security software available for smartphones is not yet as strong as that for PCs and so care should be taken with sensitive data held on smartphones.

Embedded system/Internet of Things

Embedded computer systems are everywhere. For example, cars have computers which monitor emissions from the engine and adjust the engine settings as required. Other computers check for problems with the car systems and, if so, inform the driver.

The concept of the internet of things describes a global network of connected objects, not just traditional computer networks or even robotic system but anything which could have **RFID** (radio frequency identification) chips embedded within them. With smaller and cheaper chips becoming available all the time, **connectivity** now includes animals with microchips that identify their owners and GPS location, the internal workings of the human body, movement of goods, to name but a few.

See also Unit 17 (page 352).



KEY TERMS

RFID (radio frequency identification) – tiny computer chips which hold information that is transmitted when it passes close to a scanning antenna.

Connectivity – the ability to connect with another computer or information system.



RESEARCH ACTIVITY

Identify three examples of embedded computer systems within the home and explain the advantages and disadvantages of each one.

Mainframe and quantum computers

Mainframes are huge machines designed to solve scientific and engineering problems that require complex calculations or the manipulation, collection and storage of large amounts of data.

Mainframes are reliable and secure because they have rigorous backup capabilities and component redundancy, which means if one component fails, others take its place without stopping the processing or input/output

activities. Mainframes are very expensive and require teams of experts to oversee them, and so are used only by organisations that need to process very large amounts of data quickly, such as banks, credit card companies and airlines. They use traditional bit technology, CPUs and storage which use only '1' or '0' to carry out instructions or manipulated data.

Quantum computers are still experimental. They work with quantum bits (qubits) which are not limited to two states as mainframes and PCs are. Qubits represent atomic particles, such as electrons or photons, which can be in several different states at the same time. A fully working quantum computer will be able to carry out data manipulations many million times more quickly than current computers.

GROUP ACTIVITY

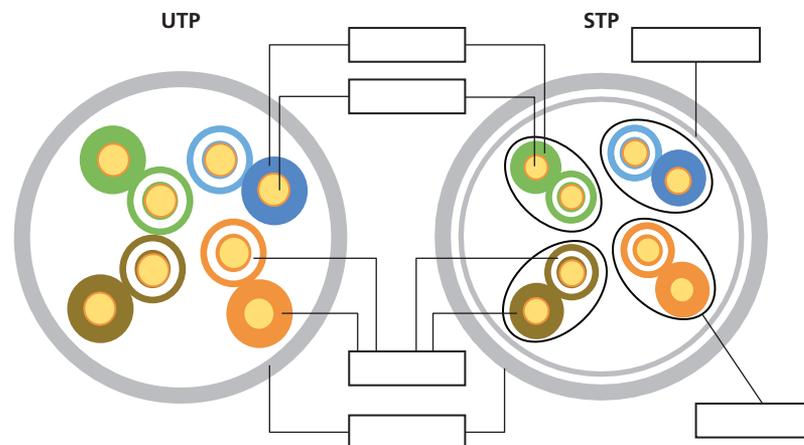
(30 minutes)

In small groups investigate types of computer systems which would meet the needs of a self-employed photographer who is going to expand his business to include another photographer and a part-time administrator, and list the benefits and limitations of each. Identify the system that you believe to be most appropriate and justify your choice.

1.4 Connectivity

Copper wire connections

Twisted pair (TP) is a common cable, often used in telephone systems. A pair of insulated wires are twisted together. Several twisted pairs can be brought together to form a twisted cable. There are two types: unshielded twisted pairs (UTP) and shielded twisted pairs (STP).



▲ **Figure 1.3** Unshielded and shielded twisted pair

The shielded twisted pair combines shielding and cancellation and wire twisting. Each twisted pair is encased in metallic jacket and four pairs of wires are wrapped in another metallic braid jacket.

GROUP ACTIVITY**(20 minutes)**

Another copper wire-based connector is coaxial cable, which you may have seen at the back of your television set, linking it to the aerial socket. Investigate the structure of the cable, as we did for the twisted wire, and identify the similarities and differences between the two types of coaxial cables: thick and thin.

Fibre cables

Optical fibres provide the fastest data delivery by cable. Each fibre is no thicker than a human hair: the thinner the fibre, the better the signal. The signal is sent down a glass rod, or core, as a beam of light, in the same way as you see in an optical fibre lamp. Optical fibre transmission is uni-directional (can only go in one direction), so at least two fibres are placed in a cable to allow bidirectional (going in two directions) transmission.

INDEPENDENT ACTIVITY**(15 minutes)**

Describe at least two strengths and two weaknesses of each cable type.

- UTP
- STP
- coaxial
- optical fibre.

Wireless technologies do not use cables but instead use radio frequency (RF) signals to transmit data or instructions between devices, including computers, printers and certain credit or debit cards and payment terminals using electromagnetic radiation. The differences tend to be the wavelengths of the RF waves.

Table 1.7 Types of wireless technologies

	Used for	Range
Bluetooth	Short-range communication between two devices without the need for a wireless network hub.	Within 10 metres.
Wi-fi	Connecting devices via a network hub.	Up to 92 metres depending upon frequency, but can be compromised by obstructions (e.g. metal or brickwork), so more than one network access point may be required.
Laser networks	Sending large quantities of data using a light beam to devices in line of sight. Also satellite to satellite communication.	Up to 10 km, but can be blocked by fog or haze as the droplets refract the light and disrupt the signal.
Infrared technology	Uses infrared LED-emitting light received by a photodiode in the receiving device, e.g. TV remote control. Cheap compared to other wireless technology and works well over short distances.	Devices must be in line of sight and only a few metres apart.
Microwave communication	Uses short radio waves to send signals via microwave towers. Can provide analogue or digital formats.	Devices must be in line of sight with no obstructions between the microwave antennae.

**CLASSROOM DISCUSSION****(30 minutes)**

Research and discuss standards, such as GSM (Global System for Mobile Communications), and associated technologies such as 3G and 4G. Use your research as a basis to discuss current developments and possible new technologies.

1.5 Communication hardware

These devices transmit analogue or digital signals over wired or wireless channels. We have already discussed the modem, which uses telephone wires to allow computers to communicate. Other examples are:

- Network hub: the central connection point for all devices in the network. All devices have equal call on the resources and receive copies of all transmissions.
- Switch: a device that receives packets (transmissions), processes them and forwards them onto the specific device.
- Router: forwards packets between networks. It needs to be linked to at least two networks, e.g. wide area networks (WANs) or local area networks (LANs), or a LAN and the network of an internet service provider (ISP).
- Hybrid network hub: includes internet access, wireless and wired LANs. They have a fixed number of ethernet ports for wired devices and also broadcast a wi-fi signal.

**CLASSROOM DISCUSSION****(30 minutes)**

Research and discuss the advantages and disadvantages of network hubs, switches, routers and hybrid network hubs.

1.6 Hardware troubleshooting

Identifying hardware faults

Faults arise for a number of reasons, such as power surges, poor maintenance, accidental damage, malware or intentional damage. The one thing you can be sure of is that faults will occur and often they have happened before. IT technicians and help desk staff must log the issue (e.g. battery will not charge, hard drive failure) on a fault log sheet identifying the:

- machine
- owner or users
- fault
- date
- symptoms
- problem history: has this happened before? Is it an intermittent fault? Has it happened to similar machines?
- Back up documentation: what has been backed up? To which location?

**KEY TERM**

Troubleshoot – the ability to analyse and solve issues with information systems.

When investigating faults:

- Always look for the simplest explanation first; for example, if the computer does not power up, check it is plugged into the mains or, if it is a laptop, plug it into the mains to see if the battery needs charging.
- Record the steps you are taking to identify the fault and confirm that you have completed a test before you start the next one. This confirms that different tests have not interfered with each other and given a false result.
- State the tools you have used to identify the fault.
- Record the actions you have taken to resolve the issue; for example, replaced hard disc, updated drivers, reinstalled software, replaced the motherboard.
- Note the product specification of any new software or hardware.
- Record the time taken and the costs arising from the fault finding and repair of the hardware.

This compiles a history of the issues with the hardware, which can be analysed to identify:

- Maintenance requirements.
- The robustness of particular hardware.
- Trends or patterns that identify which particular sets of actions result in failures, and their timescales.
- 'What if' scenarios.

Troubleshooting tools

Event viewer

When an error occurs on a computer, the event viewer is updated with information about it, including:

- what the problem is
- when it occurred, i.e. date and time
- the seriousness of the problem
- what caused the problem
- an event ID number
- who was logged into the machine at the time.

Self-test programs

These may be provided by the hardware manufacturer such as:

- Power on Self-Test (POST): a function of the BIOS for a particular computer. It checks memory, power supply, hardware, CPU, BIOS and heat/cooling. Two types of BIOS-related diagnostic information are provided:
 - Beep codes: One beep means that all is well from a motherboard perspective, as the CPU is functioning. More than one beep means that an error has been detected. Each BIOS has its own set of beep codes which can be downloaded from the manufacturer's website to identify the particular error.
 - POST codes are a visual, two-character read out of the stage that the POST is at.
- Ping tests the connectivity between the requesting host and the destination host. It uses the Internet Control Message Protocol (ICMP) to send an echo request message to the destination host and listen for a response called the echo reply message. A response shows that the host can be reached. This procedure can be repeated with different hosts until the source of the problem is identified.

**KEY TERMS**

IP – Internet Protocol short for TCP/IP which is the Transmission Control Protocol/Internet Protocol which sets the rules by which computers communicate.

IP Address – the way in which devices communicate via the internet. It consists of four numbers, each with a value of between 0 and 255, separated by a full stop or dot, rather like a post code and house number.

- Ipconfig/Iconfig identifies the specific **IP** configuration of the hosts affected by the problem. It is especially useful where dynamic addressing is used and the **IP address** of each host can change.
- Nslookup aids the diagnosis of issues with dynamic name systems (DNS) addresses. This utility looks up the IP addresses associated with a particular domain name such as ocr.org.uk or bbc.co.uk. If the utility cannot determine this information, there is a DNS issue. This utility can also query DNS servers to find out if there are issues with the default DNS servers.

Diagnostic software

This is available from third parties. Some are free and others require payment. They include memory testers.

1.7 Units of measurements

Computers are powered by electricity which is either 'on' or 'off'. This is represented as '1' and '0' even on home equipment such as kettles. Each one (1) or zero (0) is called a bit, which is short for 'binary digit'. However, to carry out instructions or manipulate data, these patterns of 1s and 0s need to be understandable to both the computer and the human user. Coding computer programs and data in binary is time consuming and likely to result in errors so computer scientists assigned a fixed pattern of bits to decimal numbers and characters. Binary coded decimals (BCD) were formed from a group of only four bits of an eight-bit or one-byte register. The second four bits were used for the sign of the number (plus or minus). These four-bit segments became known as a nibble.

As computers were used for many more purposes than mathematical and scientific equations, the range of numbers and characters to be encoded grew and the four bits could not provide enough unique patterns to cover upper and lower case characters, numbers and special symbols such as comma, full stop and exclamation marks. As a result, eight bits became the new version of binary coded decimal called EBCDIC. This in its turn was superseded by ASCII code (American Standard Code for Information Interchange) and now Unicode, which incorporates non-English language characters such as Chinese and Arabic.

Marketing information about computers refers to terabytes (TB), gigabytes (GB) and kilobytes (kB) of data storage. However, a new computer with its 1TB store only has about 976 GB of available storage space. This is because of the difference between a decimal thousand (1000) and the binary equivalent of 2^{10} (1024).

When computer memory was only a few thousand kilobytes, computer scientists and engineers noticed that there was only 24 bytes of difference from the decimal thousand, so they started to use the decimal unit 'kilo' as shorthand for 1024 bytes.

Unfortunately, as memory size has grown, so has the difference between the two values, resulting in a difference of about 10% when talking about tera values (which is 10^{12} and the binary equivalent of 2^{40} – see Table 1.8). It matters because the speed of transfer of the smaller decimal gigabyte of data is very different from that of a binary equivalent.

Some organisations calculate their data sizes in binary but use the decimal naming conventions. For others, sizes are calculated and named as decimals. Therefore, it is useful to know that there are different units of measurements and understand their relative sizes. For example, giga is bigger than mega but smaller than tera.

In Table 1.8, the term SI (Système International d'Unités) refers to the globally agreed system of base units of measurement. The IEC (International Electrotechnical Commission) is the body responsible for international standards of the electronic and electrical and other related technologies.

Table 1.8 Comparative units of measurement

Decimal values		Binary values	
SI	Bytes	IEC	Bytes
KB (Kilobyte)	$10^3 = 1000$	KiB (Kibibyte)	$2^{10} = 1,024$
MG (Megabyte)	$10^6 = 1,000,000$	MiB (Mebibyte)	$2^{20} = 1,048,576$
GB (Gigabyte)	$10^9 = 1,000,000,000$	GiB (Gibibyte)	$2^{30} = 1,073,741,824$
TB (Terabyte)	$10^{12} = 1,000,000,000,000$	TiB (Tibibyte)	$2^{40} = 1,099,511,627,776$
PB (Petabyte)	$10^{15} = 1,000,000,000,000,000$	PiB (Pebibyte)	$2^{50} = 1,125,899,906,842,624$

Powers of numbers mean the number of times it is multiplied by itself. Let us look at some of the powers of 10.

You can represent the word "power" in a number of ways so 10 to the power of 2 is the same as 10^2 or 10^2 or $10 \times 10 = 100$. Similarly, powers of 2 are the number of times 2 is multiplied by itself so $2^2 = 2 \times 2 = 4$.

Note: A number to the power 0 (for example 10^0) is always 1!

As you can see, the difference between a petabyte and a pebibyte is very large. You do not need to remember these numbers, but you do need to recognise the names and the number of bytes in powers of 10 and powers of 2, respectively.

1.8 Number systems

Most programming at user level is carried out using languages such as Python, C++ or Java, which are related to human language. However, for a computer to understand the instructions and manipulate the data, it has to be changed to lines of 1s and 0s. When designing new components or problem solving new programs, it may be necessary to read and interpret some of these instructions and understand how to convert one number system to another.

These are decimal, which humans work with, binary which the computer uses, and hexadecimal, which is used to express groups of binary digits (hexadecimal means sixteen bits or two bytes) as program instructions strings of text characters. These allow the human programmer to more quickly and accurately read the information provided.

For base 10 (decimal), the units are 0 to 9.

For base 2 (binary) the units are 0 to 1.

For base 16 (hexadecimal) we can only use a single character. Numbers of 10 and over are changed to letters and so, for base 16, the units are 0 to 9 and A to F, up to 16.

The position of a decimal number in a line of digits denotes its value. The further to the left, the higher the value.

Table 1.9 The value of 2,174 in decimal units

Thousands	Hundreds	Tens	Units
10^3	10^2	10^1	10^0
$10 \times 10 \times 10$	10×10	10×1	1
2	1	7	4

The value in words is two thousand, one hundred and seventy-four.

Each location tells us how many units, tens, hundreds and thousands. Number 10 is never in a column because that would move to the next column to the left. For example, adding 1 to 999 results in no units, no hundreds and one thousand.

We can take a similar approach to binary and hexadecimal. In Table 1.10, the number 238 is shown in binary notation.

Table 1.10 The value of 238 in binary notation

Decimal	128	64	32	16	8	4	2	1
Power of 2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Meaning	$2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$	$2 \times 2 \times 2 \times 2 \times 2 \times 2$	$2 \times 2 \times 2 \times 2 \times 2$	$2 \times 2 \times 2 \times 2$	$2 \times 2 \times 2$	2×2	2×1	1
Binary number	1	1	1	0	1	1	1	0

Clue: if the 2^0 is a 1, this means that the decimal equivalent is an odd number, if it is a 0 it is an even number.

1.9 Number conversions

To convert a decimal number to binary, we keep dividing it by 2 and make a note of the remainder. This remainder tells us where the 1s and 0s appear in the particular location. So to convert 215_{10} to binary (the small 10 reminds us that this is a decimal number):

$$215 \div 2 = 107 \quad \text{Remainder (R)1}$$

$$107 \div 2 = 53 \quad \text{R1}$$

$$53 \div 2 = 26 \quad \text{R1}$$

$$26 \div 2 = 13 \quad \text{R0}$$

$$13 \div 2 = 6 \quad \text{R1}$$

$$6 \div 2 = 3 \quad \text{R0}$$

$$3 \div 2 = 1 \quad \text{R1}$$

$$1 \div 1 = 0 \quad \text{R1}$$

Reading the remainders from the bottom, we have 11010111_2 .

To convert this number to decimal, we can label each 1 and 0, 0 to 7 from right to left as shown in Table 1.11.

Table 1.11 Example of binary number placement

Binary unit	1	1	0	1	0	1	1	1
Place number	7	6	5	4	3	2	1	0

This tells us the power of 2 by which we must multiply each 1 or 0. So we have:

$$1 \times 2^7 + 1 \times 2^6 + 0 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 1 \times 128 + 1 \times 64 + 0 \times 32 + 1 \times 8 + 1 \times 4 + 1 \times 2 + 1 \times 1 = 215.$$

If we look at 215, we note that the decimal value requires only 3 digits but the binary number needed eight digits. As the size of the number increases, so does the length of the binary number. For example, 1000_{10} is represented as 1111101000_2 .

Computers do not use an alphabet or grammar and so all letter and special characters such as exclamation marks, questions marks and full stops require their own group of bits. Trying to pick out issues from long lines of 1s and 0s is difficult for those involved in computer engineering and computer graphics. So step forward hexadecimal!

Remember the byte, which is eight bits, and nibble, which is half a byte? Consider the range of values which can be identified using just four bits.

$$1111_2 = 8 + 4 + 2 + 1 = 15$$

Therefore, if we count in 16s we can use these fifteen values to represent 1 to 15.

To convert the number 358_{10} to hexadecimal we divide it by 16, remembering the remainder.

$$396 \div 16 = 24 \quad \text{R12 (C) – remember, letters are used for numbers over 10.}$$

$$24 \div 16 = 1 \quad \text{R8}$$

$$1 \div 16 = 0 \quad \text{R1}$$

Reading from the bottom we have $18C_{16}$.

To convert the hexadecimal number into decimal we carry out a similar approach to that used for the conversion from binary to decimal.

Table 1.12 Example of hexadecimal number placement

Hexadecimal unit	1	8	C
Place number	2	1	0
Power of 16	16^2	16^1	16^0
Meaning	16×16	16×1	16×0

$$\text{Thus: } 18C_{16} = 1 \times 256 + 8 \times 16 + 12(C) \times 1 = 256 + 128 + 12 = 396.$$

KNOW IT

- 1 Convert the decimal number 407 to:
 - a binary
 - b hexadecimal.
- 2 Convert hexadecimal number 23F to:
 - a binary
 - b decimal.
- 3 Convert binary number 1110011 to:
 - a hexadecimal
 - b decimal.

LO2 Understand computer software

GETTING STARTED

(10 minutes)

In pairs, produce a list of the software which you use on your computer.

2.1 Types of software

There are many ways in which computer software can be classified. One way is by considering how it was developed:

- Is it copyright protected or available to all?
- Can the user make changes to the **source code**?
- Is it developed for a particular organisation or for general use by many individuals and organisations?

These differences are considered below.

Open source software

This means that the source code, produced by the programmer, is made available to anyone who wishes to debug, improve or modify it. Some producers of the original source code may restrict access and modification for all or some of the **code** but the principle is access for all.

Closed source software

This is closely guarded and can be protected by intellectual property rights and copyright, with the full force of the law being brought down upon those who flout the restrictions. When purchasing such software, you are purchasing a right to use it but you do not own it.

GROUP ACTIVITY

(20 minutes)

In small groups, describe at least two advantages and two disadvantages of open source and closed source software.

Off the shelf and bespoke software

A business wanting to replace or introduce applications such as financial planning or inventory systems may ask: 'Should we buy a general package and then use the parts we need, or is the way we work so different that we should have a package written especially for us?'

The first option is often referred to as 'off the shelf', as the package is pre-designed, and (when the term was invented) came in a box that you literally took off the shelf (these days, it is likely to be downloaded but the principle is the same). You may be able to make small adjustments, such as to colour or layout, or design forms and reports, but, overall, you may have to change some of your systems and work practices to fit the software.

KEY TERMS

Source code – code, written by programmers in a high or low level programming language, which is converted into a list of instructions for the computer to provide various functions and actions.

Code – groups of symbols, characters, words, letters or figures used to represent messages or instructions.

Bespoke software, like a bespoke suit or shirt, it is made to your exact measurements. It is expensive and takes time for the designer to identify your needs and convert them into a specification to turn into the program. The time it takes to provide a working program also needs to be considered. There may also be a discussion over who owns the intellectual property rights.

Shareware

If you are not sure what you need, you can try shareware for a period of time, often 30–60 days, before you have to purchase the product. At the end of the trial period you either pay the purchase price or the software locks you out. All intellectual property rights and copyright remain the property of the shareware author.

Freeware

Freeware is distributed free of charge, although there may be restrictions on upgrades or no warranty. All rights remain with the writer or publisher. The range of freeware products run from small, special utility programs to well-known programs such as Acrobat Reader, iTunes and MSN messenger which are available to all.

Embedded software

This is a piece of software which may be embedded in a traditional PC or devices we do not consider to be computers, such as microwave ovens, GPS systems, smartwatches and guided missile technology.

GROUP ACTIVITY



(45 minutes)

Investigate the types of software that could be used by a new small business, a clothes shop which buys stock from wholesalers and sells to the public online.

Investigate possible software options from each of the software types identified in 2.1 and explain what type of software each is and at least one strength and weakness for each example.

From this, make a final set of recommendations.

2.2 Applications software

Applications software is designed to carry out tasks such as accounts management, text creation and editing, presentation preparation and design drawing, which would be required whether or not a computer was available. They can be split into different types to aid the user in recognising the right software for a particular purpose.

Productivity software

This is designed to enable you to carry out your task or role accurately, effectively and efficiently. You have no errors (or at least can edit them out), it produces the correct outcome, in line with your instructions, and you do not waste time or resources. Examples of such software include word processors, databases, email, webinars and webcasts.

Development tools

These are software tools which help those who are creating new software for other purposes. This software could be a programming tool used to create, debug, enhance and maintain programs during their lifecycle. Examples are compilers, assemblers, disassemblers and debuggers. It could also be an application development tool which assists software developers to develop websites and mobile application tools.

Business software

This refers to software which supports one or more business activities. Business here should be considered in its widest sense, as it includes not only project management tools, CAD/CAM design packages and management information systems (MIS) but also specialist software, such as expert systems which gather specialist information for a particular area and apply it to new problems, for example medical diagnosis.

2.3 Utility software

Computers can suffer from viruses, loss of memory or slowness at some point. Utility programs are small pieces of software that can help the computer perform more efficiently or effectively. Examples include backup facilities, which remind you to back up your data in case of hardware failure, loss or theft of the computer. The antivirus utility regularly scans the computer for evidence of malware activity or presence; it also checks for new threats and removes them to a 'quarantine location' where they are held until the user confirms that they are to be deleted.

2.4 Operating systems, 2.5 Functions and 2.6 Benefits and limitations

GROUP ACTIVITY

(30 minutes)

Investigate the advantages and disadvantages of three different types of software utility and produce a presentation.

The operating system is the most important software in any computer system. It is a group of systems software which manages the resources of the computer, for example by:

- controlling the time each task is allowed in the processor
- interrupting when a more urgent task takes priority
- ensuring data is stored properly and the location recorded
- retrieving data from storage
- monitoring input and output.

It is normally supplied with the computer and may only run on that hardware (for example, iOS is only installed on Apple products). However, other operating systems such as Windows can be installed on a range of devices, including Apple products.

Operating systems differ with the role expected of them. For example, a single user operating system is found on PCs and tablets, where only one user can operate the device at a time, whereas a multiuser operating system has facilities which enable two or more users to have access at the same time.

Extra facilities are required by a multiuser operating system; for example, it must be able to prevent several users accessing the computer processor at the same time and overwriting each other's software or data. Users should not be able to 'see' each other on the system and should be unaware that anyone else is using the system.

GROUP ACTIVITY



(60 minutes)

Rashid and Anita are setting up a company to develop handheld infra-red security camera systems. They plan to monitor these systems on behalf of their clients, which will include military and defence contractors. They want to review application, utility and operating systems software to identify the most appropriate software.

Both Rashid and Anita have used computers for many years and so have heard terms such as 'off the shelf', bespoke and open source but do not fully understand what is meant by each term or indeed their strengths and weakness for a given situation.

They have asked you to report back on the pros and cons of each type of software.

- 1 In groups, work together to provide a short presentation on the types of software they could use and the relative advantages for the business.
- 2 Produce a report on the range of different software needed to run the business. Ensure you provide a justification for your choices.
- 3 The company is going to use a mixture of single and multiple processor systems. Rashid and Anita have asked for a brief presentation on the similarities and differences between the operating systems for each one. Produce a presentation covering their requirements.

2.7 Communication methods

Email, instant messaging, text messaging and Short Message Service (SMS)

These are written communications, although the introduction of emoticons recognises that some pictorial information is also communication. Email and instant messaging require internet access, whereas text messages and SMS are sent to mobile telephones via the mobile network. Many mobile devices, including tablets and smartphones, offer both internet and mobile network access and so all of these services can be accessed simultaneously through one or more service provider.

Table 1.13 Types of written communication methods

Communication method	What does it do?	How does it work?
Email	The most flexible of these methods, it enables both short messages and detailed discussions and allows the attachment of large files such as reports, presentations and images.	Sent via a mail server. Client software connects the user's computer to the mail server. Permits hyperlinks, which can take the reader directly to a particular web page. Email software can be provided with the computer, downloaded from the internet or provided by internet service providers (ISPs) that host email on remote servers.
Instant messaging	The user communicates directly with their contacts as they are both online. Messages are typed in a small window which appears on both screens.	Sent via a mail server. The software is a utility of the client software which uses a proprietary protocol (a communications protocol which has one owner) and which is not understood by other instant-messaging services so users can only talk to those on the same service (although some utilities now allow contact to one or two other services).
Texting and Short Message Service (SMS)	Both work in the same way but SMS restricts the characters in a message to about 180.	The software uses the control channel or pathway between the mobile phone and the mobile phone tower. A text message is sent as a packet of data, which includes the message and the addresses of the receiver and the short message server centre (SMSC). It is held until the receiving phone is available.

Voiceover Internet Protocol (VoIP)

This method can apply to digital telephone systems, video-conferencing and teleconferencing as well as to users with a computer, microphone and speaker system. Each has a codec (coder and decoder), which can be hardware or software. This device converts analogue sound or vision to a digital signal and carries out a reverse process by decoding the signals. To send this information, extra information is required, such as the IP address of the recipient.

The range of hardware and software is wide and a protocol (an agreed method of communication behaviours) allows them to communicate. The International Telecommunications Union (ITU) has a suite of protocols (H.323) which apply to both audio and video transmission. Other protocols, such as SIP (Session Initiation Protocol) enable mobile devices and computers to communicate over the internet using a SIP address. It requires a SIP client to be installed on the device and a SIP address, which is available from various sources. SIP and H.323 are not compatible.

Personal assistants

Personal assistants, such as Siri or Cortana, are software applications that recognise and act on voice commands. They can adapt to the user's speech, including accents, as the interaction continues. If the software cannot understand an instruction, it asks for it to be repeated or provide a pre-programmed list of commands to aid understanding.

2.8 Software troubleshooting

PAIRS ACTIVITY

(30 minutes)

Discuss the advantages and disadvantages of each type of communication and produce a table of your findings.

Troubleshooting should be a logical step by step approach to monitoring, identifying, diagnosing and correcting errors that arise. This should complement the careful recording of each step of a log of the events, which may be useful for future faults or to identify what may have caused an unexpected issue or outcome.

Common faults

Common software faults include:

- A system freeze, where the whole system locks and no key or click can release it, which may be as the result of a virus or software bugs.
- The frozen blue screen of a Windows-based system, which can be caused by issues with driver software.
- Software error or 'bug' due to poor coding or coding typing errors.
- Updates – ironically these can occur because an upgrade has not been applied and so the software malfunctions, or causes a malfunction because it has interfered with existing software.
- Unusual behaviour, such as only half a document appearing in a word-processing program.
- Software failing to load.

KEY TERM

Data packet – data is not sent as a single stream across the internet but instead it is parcelled into one or more packets, each of which has a header with additional information such as the IP address of the sender and the receiver.

Troubleshooting tools to investigate a problem

Tools and techniques which assist with software fault diagnosis include:

- Network monitors examine the traffic between computers – for example, the types of **data packets** – for errors. The system not only identifies current issues but also provides a set of benchmarks once the system is set up and stable. These can regularly be compared with the actual state of the network at a particular time.
- Virus scanners check whether malware is being run in the background and slowing down the system.

Fault finding documentation

See L01, page 14.

2.9 Protocols

Computers communicate with other devices using protocols – common rules and standards. You may already be familiar with names such as IP, TCP, POP3 SMTP and HTTP – the final 'P' usually stands for protocol.

When troubleshooting, use the process of elimination: always start with the most straightforward explanations and see if they solve the problem. For example, if the mouse cursor is working erratically, disappears or does not follow the mouse movement, it may have run out of battery power or not been plugged in. If not, move on to check if the driver is installed properly and so on.

These protocols can be grouped in various roles, as shown in Table 1.14.

Table 1.14 Types of protocol

Reason for protocol	Examples
<p>Linking computers across the internet required an agreement on how data was to be broken down and what exactly an internet address is.</p> <p>These are the oldest internet protocols and enable all types of device, brands, software and operating systems are able to communicate.</p>	<ul style="list-style-type: none"> • The Transmission Control Protocol (TCP). • Internet Protocol (IP). • UDP (User Datagram Protocol): an alternative to TCP mostly used with connections which tolerate loss and disordering of the packets sent.
<p>Ensuring the appropriate transfer of information between devices attached to the internet, including the control signals and how the data is to be structured.</p>	<ul style="list-style-type: none"> • Simple Mail Transfer Protocol (SMTP). • Post Office Protocol 3 (POP3).
<p>Dealing with how different data types should be structured.</p>	<p>File Transfer Protocol (FTP) and HTTP (HyperText Transfer Protocol).</p>
<p>Managing the network.</p>	<ul style="list-style-type: none"> • Internet Control Message Protocol (ICMP): sends messages about the condition of the network rather than the data traffic. • Simple Network Management Protocol (SNMP) obtains a range of statistics such as those for status of the CPU, memory, buffers, interface traffic and errors which it is also able to verify.

KNOW IT



- 1 List three types of software.
- 2 Name three types of utility software.
- 3 Name three voice-based communication methods.
- 4 Describe five popular protocols.

LO3 Understand business IT systems

GETTING STARTED



(10 minutes)

In pairs, list the types of networks that you use or have used – at home, at school or college and in the workplace.

3.1 Types of servers

A server is normally considered to be a powerful computer or device which serves a particular need for a network. It can also be a piece of software that operates on a network device. While almost any computer can act as a server, it requires extra memory and computing power to run both the computer and the needs of the rest of the network. Specialist servers carry out one particular service for the network.

The most common servers are the following.

File

A file server is useful for businesses or individuals who need to hold and manage large numbers of files. It stores files, indexes them, remembers where they are to retrieve them and takes responsibility for security of the

files, ensuring that only those who are entitled to read them can do so and only those who have the rights can edit or delete them. A further role for the file server is to ensure that backups are made at an agreed time, so that data can be restored if there is an accident or disaster.

Print

Print servers manage the printing of documents. They control printers on the network, allowing a group or groups of employees to send print requests to specific printers. It can also reroute print requests, if there is a fault or incident, to the nearest appropriate and available printer. It can manage the electronic print queue by sharing the load across the available printers.

Application

Application servers are designed to install, operate and monitor the applications shared by other devices on the network. Although all users share some applications, such as word processors and email, the server also manages security of restricted access applications such as financial and human resource software.

Database

Some application servers may have a specialised role as database servers, which manage databases with multiple users. These servers are database-architecture independent – the server will manage all activities, whether it is a relational database, flat file or object-oriented.

Web

A web server can also refer to hardware or the web server software. It is an internet server that reacts to HTTP requests to deliver content and services from a client.

Mail

A mail server or a mail transfer agent (MTA) is software or a device which acts as an electronic post office. It receives emails from users on the network, both in the same domain and from external senders, and forwards it to the recipients, who may be local users or external senders. For external senders, the mail server passes it to the mail server of the recipients' domain. Normally, mail servers use SMTP to send the mail and POP3 or IMAP to receive it.

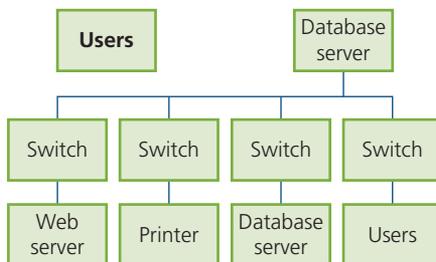
Hypervisor

This is software written for a particular processor which manages different operating systems or copies of the same operating system on a single computer or computer system. It manages resources such as the processor, memory and devices so that each operating system not only receives the resources it needs but also prevents it clashing with the other operating systems. See also L03.2.

3.2 Virtualisation

Virtualisation is to create a simulated or virtual network, computer or server using software.

Server virtualisation is not new; it has been used in mainframes since 1970s. Normally the operating system and hardware are closely linked so that



▲ **Figure 1.4** An example of a print network with different servers attached

only some applications can run simultaneously to prevent problems such as registry conflicts. To operate additional applications, additional physical servers need to be installed, possibly running only a single application. Server virtualisation enables a single physical server to run several applications, each appearing to have its own server.

Storage virtualisation works in a similar way by separating the physical storage server from the logical storage server. It can take two forms:

- Block-level, which allows a storage area network or SAN to use numerous storage arrays across the network as if they were a single array.
- File-level, which allows network attached storage (NAS) and removes the link between the data items and their physical locations on a particular file server.

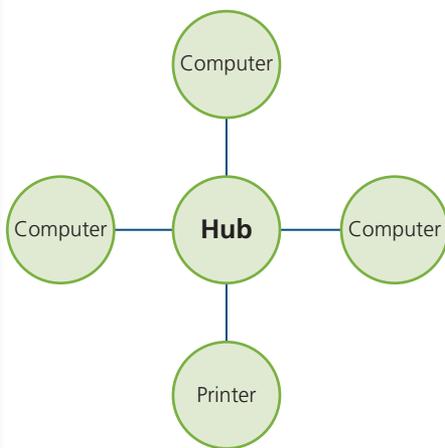
Cloud computing is not virtualisation. The cloud uses existing technology to deliver services, such as security, storage and data manipulation, to users over a network. It is used like a utility – you can increase the size or range of your usage through payment.

Hybrid cloud computing is a mixture of private cloud, public cloud and locally owned services. As its activities and data requirements change, so the organisation can adjust its usage more effectively and efficiently.

GROUP ACTIVITY

(45 minutes)

In small groups, investigate the advantages and disadvantages of virtualisation and give a presentation on your findings.



▲ **Figure 1.5** A star network

3.3 Networking characteristics

Types of local area networks include the following.

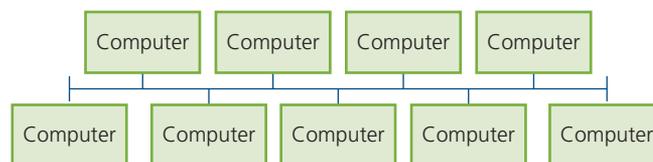
Peer-to-peer

Each computer is linked to one or more computers directly rather than going through a server. There are several forms of peer-to-peer networks.

The star network

All computers communicate through the central hub. All transmissions received from a peripheral on the star are broadcast to all peripherals by the central device. The benefit is that if one peripheral goes down the rest can continue to communicate; however, if the hub goes down the whole network is compromised. The cost of the cabling can also be expensive if the network is extensive.

Bus network



▲ **Figure 1.6** A bus network

Here, the peripherals are attached to a single cable with terminators at each end.

The advantages include:

- attaching a new device is easy, so if one peripheral fails the others are not affected
- it is cheaper in cabling terms than a star network
- transmissions are in both directions
- transmission is more likely to be read as it is received by all devices relating to the recipient.

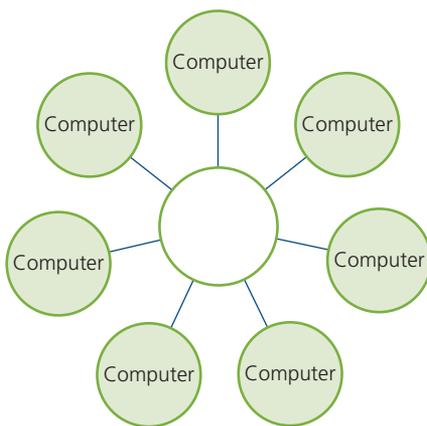
The disadvantages include:

- the difficulty of identifying a faulty peripheral
- if the cable should break either the whole network may be lost or it may split into two
- adding additional devices can slow the network down significantly
- the possibility of the transmissions crashing into each other.

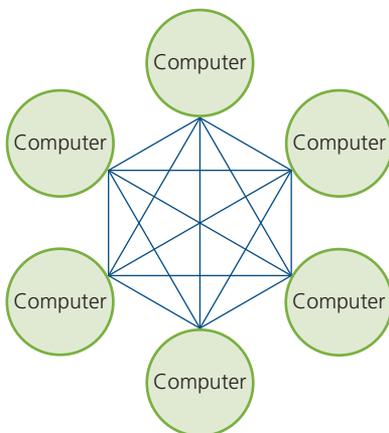
Ring network

Ring networks have one directional communication through a cable. The message is received by each computer in the ring between the sender and receiver. Each computer in the chain sends the data packet to the next computer until the receiving device receives it. Often the message is boosted or regenerated to maintain signal strength.

Rings use a method known as token passing to prevent problems of multiple messages on the network colliding. A small data packet known as the token is continuously transmitted around the ring. When a device has data to transmit, it has to wait until the token arrives. At that point, the computer checks to see if the token is already being used by another device. If not, it adds its own data and control information such as the address of the receiving device and sends the token on its way. When the notice of safe delivery is received the token is released back to the ring.



▲ Figure 1.7 A ring network



▲ Figure 1.8 A mesh network

Mesh network

There are two types of mesh network:

- Total mesh topology where every **node** (connection) in the network is connected directly to all other nodes. If a connection stops working all the traffic on the network can be rerouted around the problem.
- Partial mesh topology has some nodes connected to only a small number of nodes whereas others are connected to all the other nodes. This reduces the rerouting options if a connection fails, but it is cheaper than the total mesh because there is less cabling, for example.

Cabled mesh networks are very costly because of their complex cabling requirements but wireless mesh networks are cheaper because they do not need cabling.

Client server

In the networks identified above, all the devices are independent in that they carry out their own tasks with their own software. They may share data but not applications. Client server networks are different. One device, which may be a computer or a specialist server, provides services such as applications, storage or internet connections to its clients (the other computers in the

KEY TERM

Node – a connection, redistribution or end point on a network; anything with an IP address.

network). Larger networks may have several servers, as shown in Figure 1.4, providing different services.

It is possible to link networks through switches, gateways and routers, to allow for greater flexibility.

The choice of topology will depend upon a number of factors:

- The number of computers to be networked.
- The spread of the network, e.g. room, building, city, country or continent.
- The cost of the topology, e.g. a bus topology is cost-effective in a single room with only a few devices. A star topology with a central hub running an ethernet system is a reasonable approach for several devices and servers, as long as they are within a single building or in buildings on a single site.
- The amount of money available.

3.4 Connectivity methods

LAN

Token ring local area networks (LANs) were discussed in LO3.3.

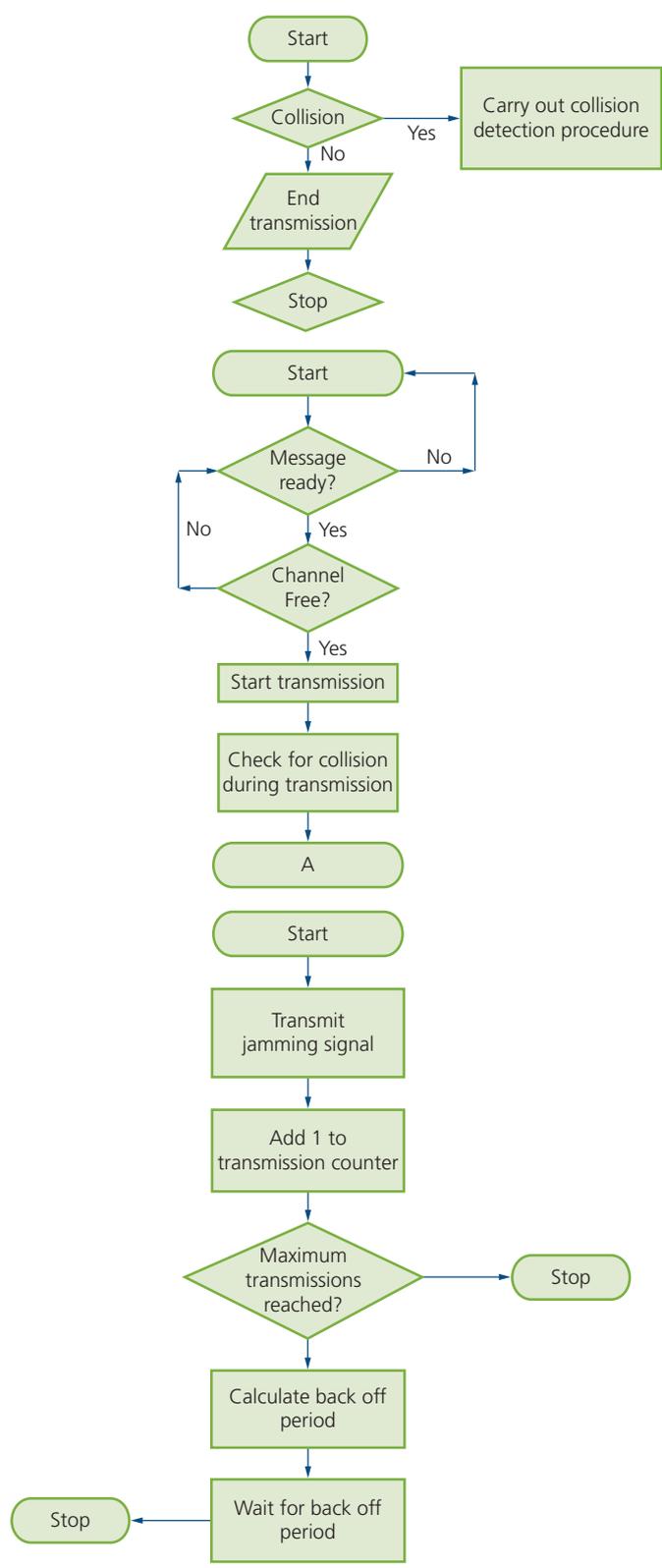
An alternative is to use an ethernet network LAN. The cabling allows messages to travel in either direction, unlike token ring networks which only communicate in one direction. Half duplex ethernet LANs allow communication in both directions but only in one direction at a time. However, if two messages are simultaneously placed on the network and crash into each other, this may bring the network down.

To enable the network to recover from this problem, a media access control (MAC) method called Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is used. It works as shown in Figure 1.9. Back off is the randomly calculated time that a device will wait to try to resend the message (the time it will back off from transmitting). Each device carries out its own calculation and so, in theory, only one will be ready to transmit once the collision is cleared.

WAN and MAN

A wide area network (WAN) can be transglobal, or cover whole countries or continents. Networks operating over smaller distances such as a town, city or cluster of close cities are called metropolitan area networks (MANs). Each type of network has its own rules or protocols to ensure that generic devices can communicate.

Examples include ASDL (asymmetric digital subscriber), which supports faster transmission of data over the copper wire telephone lines than the traditional voice modem. ISDN (integrated services digital network) is a set of standards for digital transmission of data, video and voice over traditional telephone copper wire. Leased lines, rather than operating through national and international telephone wires, provide a fixed-bandwidth data connection. This means that the bandwidth is only available to the leasee, avoiding a slowdown in transmission when the network is busy.



▲ Figure 1.9 Transmission of message using half duplex ethernet

Voice

Data and voice communication can be sent over telephone wires or by cellular or satellite technology. The clearest and most reliable method is over fixed cables between the sender and receiver. If it is not possible

to be linked to a handset or computer which is plugged into a public switched telephone network (PSTN) (e.g. while travelling or in remote parts of the world), cellular (mobile phone) and satellite communication is appropriate.

However, cellular technology requires the towers which carry transmitter/receivers to be in line of sight to the user's communication device. Disappearing into tunnels on a train, standing in a remote field or being shielded by large buildings can disrupt this point-to-point communication. Also, providers do not like to share their communication systems with other providers as they risk losing revenue from new customers.

Satellites

Satellites in geostatic orbit (those that appear to stay in a single location over Earth) are point-to-multipoint communication systems as they receive transmissions and rebroadcast them to receivers. If required, the satellite can be moved to another location relatively quickly. However, the distance between the satellite and the ground, normally about 75,000 km (46,603 miles), means there is a delay between the transmission of the signal and its receipt, which can be seen on television news reports from remote locations. Data transmission is also compromised by this issue, especially when trying to transfer large files.

3.5 Business systems

Businesses have developed many systems to manage and manipulate data and aid business practices.

MIS

Management information systems (MIS) refers to the software and hardware used by managers to obtain the necessary information for accurate decision-making and monitoring the effectiveness of decisions. The system continuously gathers internal and external data, and refines and organises it in one or more databases where it can be interrogated by those with access rights. The data can be downloaded, for example for:

- reports and other documents
- spreadsheets and strategic decision support systems
- functional systems such as those for marketing, sales or production.

Used wisely, an MIS can provide evidence of:

- the status of the organisation
- areas of improvement, e.g. rising sales
- areas of risk, e.g. falling sales, loss of market share
- personal or group responsibility for success or failure.

Limitations of MIS systems are:

- cost of creating and installing the system
- poor or inflexible design which does not meet current or future needs of the organisation
- data that is out of date, incomplete or incorrect because of poor error checking facilities

- end users who do not use the system properly; this is often caused by lack of training
- it does not make judgements; it only provides the information needed for decisions.

CRM

To ensure that customer needs are met, data must be gathered, analysed and shared. Customer relations management (CRM) is a process that tracks how the business interacts with current and potential customers. A computer-based CRM system supports such activities by holding records of client communications, meetings and documents. This information is available to those with access rights.

A CRM system allows a business to centrally hold customer information such as:

- contact details
- customer histories
- leads for new customers
- leads for new services.

Although CRM is primarily aimed at sales and customer support functions, marketers also use CRM to aid their understanding of current sales, prospective sales and forecasting future trends.

Limitations to CRMs include:

- Software issues, such as limits on data storage size or emails.
- Integration difficulties with other organisational systems.
- Lack of training leading to poor data entry and incorrect data.
- Resistance by sales staff who believe that using digital information rather than face to face meetings with clients reduces their ability to understand subtle communication behaviours.

SOP

Standard operating procedures (SOPs) are detailed step-by-step guides to how functions should be carried out within an organisation to ensure that they are carried out accurately and in the same way each time. The outcomes from each activity should always be the same, leaving an audit trail in case of disputes or external investigations by regulatory bodies. SOPs should also be created for business systems such as those outlined above, to ensure that the data and resulting information remains accurate and useful. Software can aid the production of SOPs.

Limitations of SOPs include:

- Imposing restrictions and details which result in inflexible practice and a lack of innovation.
- Too much time being spent on the admin rather than doing the job.
- The necessity of updating the SOP to reflect new statutory or regulatory requirements.
- Lack of version control. If updates to the SOP are not recorded with a date and a brief statement about the changes, individuals could be working to different versions, which can cause serious problems.

Help desk

When a user of a large, complex or widely spread system has a technical problem, it is useful to have a knowledgeable person ready to solve it. For straightforward problems, instructions can be given to the user and the issue resolved immediately, but complex problems can be actioned by a technician visiting the location and resolving the problem or providing a temporary fix. This is normally managed through agreed levels of support for departments or customers.

Limitations include:

- Cost of setting up an in-house help desk with hardware, software and staffing.
- Cost of buying help desk services from an external source (third party).
- Issues with availability of the help desk, for example, the need for 24-hour call out; availability during bank holidays.
- Loss of service through breakdown of communication systems.

KNOW IT



- 1 Identify three types of server, one of which must be virtual.
- 2 Identify three network topologies that could be used in a small business.
- 3 For each of the purposes below identify the most appropriate business system.
 - a Support for an end user whose computer has crashed.
 - b A system to improve sales to your clients.
 - c An audit trail of actions taken by staff while carrying out risk assessment on a computer system.
- 4 Define virtualisation.

LO4 Understand employability and communication skills used in an IT environment

GETTING STARTED



(20 minutes)

Imagine you work as a software developer. Identify what communication skills you think you need and explain why they are important.

4.1 Communication skills

Working in the IT industry requires communication skills because individuals need to work independently and in teams, and provide support to, or acquire information from, those without any technical knowledge.

Interpersonal skills

Face-to-face communication involves more than just talking. You must also provide a positive image of yourself, your colleagues and your organisation. Think about what makes you take an instant like or dislike to someone when you first meet them. Signals may be through eye contact (e.g. looking directly at the person to whom you are talking, not allowing your eyes to wander) and body language. Depending on the circumstances, folding your arms and slouching rather than sitting up on your chair can give the

impression that you have no interest in what is being said or done. Some body language can be considered insulting, such as yawning when someone is talking to you.

Verbal communication

This needs to be effective and appropriate for the situation. You must know when to use technical or specialist terms and when to provide simple explanations in easily understood English. Some communications are formal, such as in meetings, while others may be more informal, such as working with close colleagues. Therefore, the language needs to be adjusted, for example, 'Hiya mate!' may be acceptable when speaking to a peer but not to senior colleagues or customers.

Questioning techniques

When trying to help those with IT problems or find out what is required, e.g. for a new system, careful questioning should help to acquire the information needed. Types of questioning techniques include:

- Closed questions, where the answer will be one word or a very short factual answer, e.g. 'Do you want a drink?' or 'How many days are there in November?'
- Open questions, where there is no obvious answer or where opinions are required, such as 'How did she react?', 'Why did you select that laptop?'

Avoid leading questions, e.g. 'Is the computer always this slow to start up?'

Written communication

It is important to distinguish between formal or informal written communication. Formal communication might be a letter of application for a job, while informal written communication is usually more casual and spontaneous, e.g. text message or email to a friend. Whether something is formal or informal will depend upon:

- The organisation's policies on documentation layout.
- Whether the communication is between colleagues or external bodies.
- Whether the communications have legal status.

You should become familiar with the business's policies and procedures for written communication, such as the format of reports, letters, emails and social networking.

Barriers to communication

Some circumstances prevent the message being given or received. They can include:

- Noise: both physical noise, which makes listening difficult, or noise in your own head generated by worries or concerns, which results in loss of concentration on the conversation.
- Language: this can be due to the inappropriate use of complex or technical terminology.
- Physical barriers such as deafness, where sign language or clear enunciation for lip reading is required to ensure successful communication.

4.2 Communication technology

Communication is aided by a range of technology – some forms are written and others are verbal.

- Presentation software can include text, graphics, video and audio images and is used to tell a story or used to support someone presenting information.
- Word processing – used for the production, editing, printing and storing of text on a computer, e.g. writing letters, reports, books, leaflets and posters.
- Email – the distribution of electronic messages from one computer user to another via a network.
- Web – a system of internet servers that support specially formatted documents often connected via hyperlinks.
- Blog – a regularly updated web page run by an individual or small group taking the form of a personal journal which is accessible to the public.
- Vlog or video log – a form of blog which includes video clips.
- Instant messaging – a communication service which enables a person to communicate privately with another individual in real time over the internet.

GROUP ACTIVITY

(20 minutes)

What communication technology would you use if you worked as a computer support technician for a small PC repair company? Justify your answers.

4.3 Personal attributes

These are the qualities individuals have which enhance their technical skills and make them useful employees.

Table 1.15 Personal attributes in the workplace

Attribute	Meaning	Possible role type
Decisiveness	Understands that difficult decisions have to be made in a timely manner, to protect the organisation or individual.	Leader
Punctuality	Demonstrates responsibility, dedication and a willingness to take personal responsibility.	All job roles
Self-motivation		
Leadership		
Respect		
Dependability		
Problem solving		
Determination		
Independence		
Time management		
Punctuality		
Team working		
Written numerical and verbal skills		
Planning and organisation skills		

PAIRS ACTIVITY

(30 minutes)

Complete the table, briefly explaining why each attribute is useful and any particular roles to which the attribute would apply. The first two have been completed for you. Copy it onto a piece of paper if you need more space for writing.

4.4 Ready for work

Present an image that says that you are prepared for work, which includes being ready to represent the organisation to any visitors and to show the importance of personal presentation. Examples include the following.

- Dress code – some organisations have dress codes that require a uniform or a dark suit, while others may be happy if everyone arrives in t-shirts and jeans. Whatever the code, employees must dress appropriately for the situation.
- Presentation – clean clothes and good personal hygiene help to give a professional impression, as others need to feel comfortable when working closely with you. Good grooming shows respect for the organisation and colleagues.
- Attitude – someone with a ‘can do attitude’ is positive about their ability to achieve success, even if things are not going well. Someone who has a responsive attitude readily accepts change and is open to suggestions made by others.

4.5 Job roles

From chief information officer to trainee help desk operator, all roles require certain attributes and skills.



CLASSROOM DISCUSSION

Find examples of job descriptions, attributes and skills for the following IT job roles:

- network manager
- IT technician
- programmer
- web designer
- animator.

Discuss why particular attributes and skills would be appropriate for each role.

4.6 Professional bodies and 4.7 Industry certification

Anyone can claim to be an IT specialist; unlike the medical or teaching profession there is no requirement to be registered or to undertake particular qualifications. However, professional bodies such as the British Computer Society (BCS), which is also the Chartered Institute for IT, seek to raise the status of the IT professional. It sets standards of behaviour and supports IT professionals in achieving recognition of their qualifications as well as skills developed through working in the industry. Professional bodies provide a number of benefits such as:

- building a network with like-minded professionals
- identifying career opportunities as many advertise job opportunities
- continuous professional development opportunities through seminars, special interest groups, journals and qualifications.

Disadvantages include:

- cost – fees can be several hundred pounds
- time – attending meetings and events for general or specialist group or local branch meetings
- does not guarantee that you will have a better job or earn more money.

Training includes certificated courses which provide the individual with national and/or international recognition of the level of knowledge, understanding and experience in certain areas of IT. They also provide the opportunity to achieve new skills and knowledge for future roles.

CLASSROOM DISCUSSION

Look at a range of industry awards and the bodies who offer them, such as CISCO®, and consider:

- What is the purpose of each award?
- How does achieving the award benefit the individual?
- How does employing staff who hold the award or providing opportunities to study for them support an organisation?

KNOW IT

- 1 What interpersonal skills would you use when communicating with a client on how to set up their email account?
- 2 Suggest two methods of communication technology that could be used to create a user guide on how to install a wireless printer.
- 3 What personal attributes would you need for this role?
- 4 You are working as part of a team developing bespoke information systems for businesses. Some of your colleagues are working on a project and need help as they have very short deadlines and are concerned that they will not meet them. What attitude would you show to your colleagues?
- 5 Give two advantages and two disadvantages of being a member of a professional body.

L05 Understand ethical and operational issues and threats to computer systems

GETTING STARTED

(15 minutes)

Computer systems are open to a number of threats. In pairs, discuss and identify as many threats as you can to computer systems. These can be for standalone computer systems for a single user as well as computer systems which are part of a network.

 **KEY TERM**

Whistle blowing – making a disclosure that is of public interest.

5.1 Ethical issues

Whistle blowing

Whistle blowing is usually when an employee discloses that some form of serious unlawful practice is taking place within their place of work. The activity could include miscarriages of justice, illegal activity, threats to individuals and/or damage to the environment. Whistle blowers are protected by UK law against any form of ‘punishment’ by their organisation, for example, unfair dismissal or not being promoted.

Disability/gender/sexuality discrimination

Behaving ethically can be underwritten by law; for example, the Equality Act (2010) ensures equality of treatment for all people, irrespective of colour, race, disability or gender. These and other characteristics are classified as protected. Examples of discrimination could be people not receiving equal pay for the doing the same job because of their gender, disability and/or sexuality.

Use of information

The Data Protection Act (1998) ensures that personal data is used responsibly. When designing, developing and/or using information systems, ethical considerations should be made with respect to how the information is collected, processed, stored, used and distributed.

Codes of practice

There are many codes of practice within the workplace to provide ethical guidance. An organisation may have a **code of practice** for confidentiality in relation to its clients, for example, so if you saw confidential information while developing an information system you would be bound by your organisation’s code of practice not to share any of the information you have seen. There are codes of practice for **ethics** (how you behave), quality assurance (how the organisation ensures that quality is maintained with respect to the products and/or services it provides), equality and discrimination (being fair and objective with advice and actions provided to employees and clients).

Staying safe online

There are guides on staying safe online to avoid problems with individuals who do not behave ethically or perhaps have a different ethical code from those of society as a whole. See Unit 3 for more details.

5.2 Operational issues

These cover a wide range of circumstances that could jeopardise individual departments or the entire organisation. Some examples are as follows.

Security of information

Failure to protect information from loss, corruption, illegal duplication, or being stolen, manipulated or hacked can provoke poor publicity, which can result in loss of business, bankruptcy or even fines and court cases. Loss of production information and sales data can leave a business unable to meet its requirements.

Health and safety

Failure to protect employees and clients or visitors can reflect badly on the organisation if reported in the press. It can also result in large compensation

 **KEY TERMS**

Code of practice – a set of rules which explains how people working in certain professions are required to behave.

Ethics – the accepted behaviours and beliefs of society or groups within it which influence how people react to situations.

claims, court cases, fines or even imprisonment in the most serious instances, such as loss of life. There is also an ethical or moral issue, as risking the lives and health of employees through a careless attitude to their safety is not acceptable behaviour.

Disaster and recovery planning

Organisations take note of all the issues that could risk their assets, employees and existence. They will produce a plan to either reduce the risk to the lowest possible level or provide alternative facilities or locations. For example, backing up computer data as often as necessary will ensure that minimal data is lost if there is a computer failure. Placing copies of the backup data in different physical locations in case of fire, flood or earthquake is also a possible disaster plan.

Organisational policies

Organisations have policies to establish the rules for acceptable behaviour and guidelines for best practice in certain work-related situations. An acceptable use policy stipulates what a person can and cannot do when using the network and/or internet while at work. Schools and colleges usually require their learners to sign an acceptable use policy before they will issue them with a network ID. A code of conduct policy sets out the standards of behaviour expected from employees while working on the premises or the premises of their clients.

All organisations need to change over time because of different factors which include the following.

Change drivers

These are things which must change, such as new legislation, new entrants into the market, an increase in the number of platforms that can share, distribute, license or sell music, or new business practices.

Scale of change

This reflects the needs of the business, such as replacing a slow network with a faster optical fibre system, introducing an extranet or allowing customers to log into some systems externally. It also provides remote access for employees so that they can access work from home.

5.3 Threats

Security covers the identification of threats like:

- Phishing: misleading individuals or organisations into parting with their confidential and personal data to commit fraud.
- Hacking: not all hacking is external, as employees also hack their own company systems. This includes looking at files or locations to which they do not have right of access; creating, modifying or deleting files without permission; or defacing web pages.
- Trojan (horse): introducing a piece of code which, when certain conditions are met, will carry out an action which will be detrimental to the system, e.g. wiping data.
- Interception: when the data packets on the internet are intercepted by a third party and copied, edited or transferred to a new location.
- Eavesdropping: can refer to interception, but is particularly listening to communication traffic not intended for the reader or listener such as email, instant messaging, faxing or video-conferencing.

- Data theft: illegally removing copies of personal or company data from information systems.
- Social engineering: the manipulation of individuals to trick them into giving sensitive information, for example, claiming to be from the IT department and asking for a password and username to check whether the PC has a virus.

To protect against these and other attacks a range of security measures is available. Normally, these are broken down into physical security and digital security.

5.4 Physical security

Examples include:

- Locks and keypads for preventing access to computer rooms or storage facilities or to prevent access to hard drives.
- Biometric readers are electronic devices to determine a person's identity. They can do this by detecting fingerprints or eyes and matching them to records in a database.
- Radio frequency identification (RFID) uses radio waves or electromagnetic waves to identify and track individuals, animals and items of importance.
- Tokens, small hardware devices, such as a keyfob or a smart card, which allow a person access to a network (for example, the tokens sent to customers by some banks to access online banking services).
- Privacy screens to prevent the content being seen or read by anyone not sitting in front of the screen.
- Shredding or cutting up documents and optical discs into sufficiently small pieces that it is impossible to reconstruct them. This is one of the most effective methods of protecting physical data no longer required from falling into the wrong hands.

5.5 Digital security

Examples include:

- Anti-virus and anti-spyware are both programs that protect the computer system from other programs which are maliciously downloaded. Anti-virus means that the software identifies and quarantines or destroys computer viruses. Anti-spyware carries out a similar role with spyware.
- Usernames and passwords provide protection at two levels. The username is linked to a group or groups. These groups allow access or give permission for the user to access particular software such as financial systems or HR. The password can allow the user access to the information system and software such as internet access, word processor, spreadsheet and email. Further passwords may be required for particularly sensitive data.
- Firewalls are used to prevent unauthorised access to or from a network. They can be implemented via hardware, software or both. Firewalls filter the traffic that flows into a PC and/or network through an internet connection and block anything that it deems harmful to the computer system or network. There are three types of filtering mechanisms:
 - Packet filtering – the firewall analyses the 'packets of information' (i.e. data) and blocks any unwanted or offensive packets.
 - Proxy – the firewall takes on the role of a recipient and sends the data received to the node that had requested the information.

- Inspection – the firewall marks key features of any outgoing requests for information and checks for the same key features of the data coming into the computer system/network, deciding whether it is relevant.
- Permissions – rules that determine who can access an object and what they can do with it. An example would be the permissions granted to people to access a shared file on a network system; so some people may only have read-only rights, while others will be able to edit the file as well.
- Encryption is when data is encoded (converted into a coded format), so that it cannot be understood by people who are not authorised to see it. The only way that someone can read encrypted data is with a secret code or key.

5.6 Safe disposal of data and computer equipment

Legislation

A range of legislation covers the disposal of data and computer equipment. These include the Waste Electronic and Electrical Equipment (WEEE) directive, which makes clear that the computer equipment needs specialist knowledge and tools to ensure safe dismantling. The UK's Waste Acceptance Criteria (WAC) deals with the disposal of monitors, for example. The Hazardous Waste (England and Wales) Regulations 2005 also applies as mercury, hexavalent chromium and other toxic chemicals found in computer systems.

The Freedom of Information Act (2000) and the Data Protection Act (1998) contain clear legal requirements for the safe destruction of data.

Overwriting data and electromagnetic wipe

These are ways of removing data from hard discs. Overwriting is when data is sent to the disc and this overwrites the '1's and '0's already on the disc. Unfortunately, once is normally insufficient to remove all evidence of the existence of the data. The process must be repeated several times and even then very sophisticated forensic techniques can often retrieve some of the data.

Electromagnetic wiping involves the use of a degausser which has a very strong permanent magnetic or an electromagnetic coil. This method can also destroy the disc itself if great care is not taken, but it does remove the data.

Physical destruction

As seen in L05.4, physically destroying hardware containing data by shredding can be effective. Some businesses provide secure bins for confidential information, the contents of which are destroyed.

KNOW IT



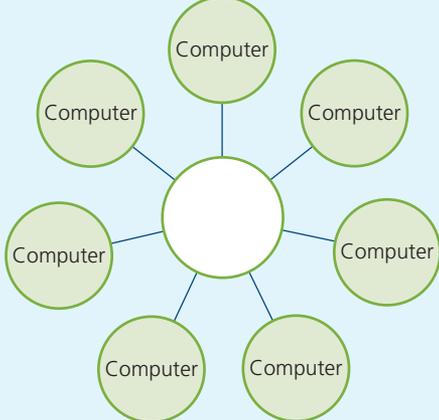
- 1 What is a whistle blower?
- 2 An organisation is concerned that if the server was to break down, they may lose their data. What operational issue would they need to consider?
- 3 What does RFID stand for?
- 4 Give two examples of how permissions could be used as a digital security method on a network.
- 5 Identify two ways in which data can be securely removed from a hard disc.

Assessment practice questions

Below are practice questions for you to try.

Section A

For each question, put a tick in the right hand column of the table to show the correct answer.

- Which of these items is ordered correctly, from the smallest to the largest? (1)
 - gibi, tebi, kibi, mebi, pebi
 - gibi, kibi, mebi, pebi, tebi
 - kilo, mebi, gibi, tebi, pebi
 - kilo, gibi, mebi, tebi, pebi
 - Which of the following is **not** a computer component? (1)
 - RAM
 - keyboard
 - power supply
 - sound card
 - Which of these is a business system? (1)
 - SOP
 - MOP
 - DOP
 - LOP
 - Which of these is an ethical issue? (1)
 - biometrics
 - encryption
 - use of information
 - security of information
 - Which of these is **not** a threat to computer systems? (1)
 - bias
 - interception
 - eavesdropping
 - social engineering
 - Which of these is a disadvantage of using the cloud for storage? (1)
 - usability
 - cost savings
 - accessibility
 - disaster recovery
- 
- Which topology is shown in the diagram? (1)
 - client server
 - ring
 - mesh
 - star
 - Which type of network is often connected through public networks, leased lines or satellites? (1)
 - WLAN
 - WAN
 - MAN
 - PAN
 - Which protocol is used to automatically provide IP addresses to network computers? (1)
 - IGMP
 - ARP
 - DNS
 - DHCP
 - Is the following statement **TRUE** or **FALSE**? (1)
Freeware is computer software that is available free of charge and has no restrictions on redistribution for which source code is not available.
 - Which of the following shows the conversion of 124 in decimal to binary? (1)
 - 00111010
 - 01010110
 - 11111000
 - 01111100

- 12** Which of the following shows the conversion 11100010 to decimal? (1)
- 220
 - 226
 - 210
 - 216
- 13** Which of the following shows the conversion of 250 to hexadecimal? (1)
- FB
 - FH
 - FA
 - FE
- 14** Which of the following is an example of digital security? (1)
- biometrics
 - interception
 - RFID
 - encryption
- 15** Which type of virtualisation is the sharing of computer resources, software or data through the internet? (1)
- network virtualisation
 - server virtualisation
 - storage virtualisation
 - cloud virtualisation

Section B

Grab and Go is a fast food outlet with six branches across the Northwest of England. This growth has taken place over the past three years and each branch has its own computer network which links via email to the others. All sales and financial records are sent weekly via email to the head office, which is the site of the original outlet.

The owner has decided that the organisation needs a network that will link the shops electronically and enable all data relating to the business to be stored centrally on a server at head office. You have been asked to work with a local IT consultant to design the new system.

- 1 Explain two advantages and two disadvantages of using a multiple processor system to run the system. (1)
- 2 The IT specialist has suggested that, rather than a server at head office, the data should be held in the cloud. The owner asks you to compare the two options so that he can make a decision. Compare the use of a server to store company data compared to using a cloud service. (6)
- 3 Draw a possible topology for a network to join the individual computers into a single wide area network. You should label all of the hardware technologies involved. (8)
- 4 Outline three ways in which the wide area network could be connected. (6)
- 5 Evaluate the use of a barcode reader system in reducing errors and updating the stock levels across the outlets. (6)
- 6 The IT consultant has recommended that Grab and Go purchases bespoke software to run its stock control system. You believe that shareware programs could be used instead. Explain the difference between the two types of software. (5)
- 7 With the introduction of a new computer network, the IT consultant has suggested that a network manager should be appointed. As an IT technician, you feel that this is an opportunity for you to obtain a promotion.
 - a Explain the personal attributes that are required for both roles and what evidence you could provide of current attributes. (3)
 - b Outline the additional personal attributes required by the new network manager. (3)
- 8 Explain why Grab and Go should undertake a disaster planning and recovery event to protect its data. (4)
- 9 Describe three threats against which Grab and Go should protect itself. (6)
- 10 Explain three physical security methods which should be implemented by Grab and Go to protect its computer systems. (6)
- 11 Explain how Grab and Go should dispose of its old computer systems and the data held on hard discs safely and why this is important. (8)