AQA AS ICT INFO2 Revision Guide (2008/10)

Living in the Digital World

DAVID J ASTALL

ict@zigzageducation.co.uk
www.zigzageducation.co.uk

POD 2845

Contents

Introduction

In this resource the main elements of each unit, according to the AQA AS Level ICT specification (2008) INFO1, are incorporated and divided into sections. The sections are numbered 2.1-2.9, but should you require them, the full AQA unit references from the specifications can be found listed on the following page.

This resource is designed to allow the learner to revise from one section at a time, while on the move carrying minimal paperwork.

The Revised box below is for the learner to TICK (✓) once the unit has been revised and fully understood.

Also available from ZigZag Education by this Author are further resources for AQA AS Level ICT. The INFO1 Revision guide, to accompany this resource, and the INFO1 Practical Work Guide, which shows students the detail of what work is required for the analysis and testing sections for the practical work.

Revision Checklist

AQA Unit	Revised	Topic
3.2.1	☐	An ICT system and its components
3.2.2	☐	Data and Information
3.2.3	☐	People and ICT systems
3.2.4	☐	Transfer of data in ICT systems
3.2.5	☐	Safety and Security of ICT systems
3.2.6	☐	Backup and recovery
3.2.7	☐	What ICT can provide
3.2.8	☐	Factors affecting the use of ICT
3.2.9	☐	The consequences of the use of ICT

2.1 – An ICT system and its components

This section looks at what ICT is; the difference between a system and an ICT system and finally looks at the components of ICT system.

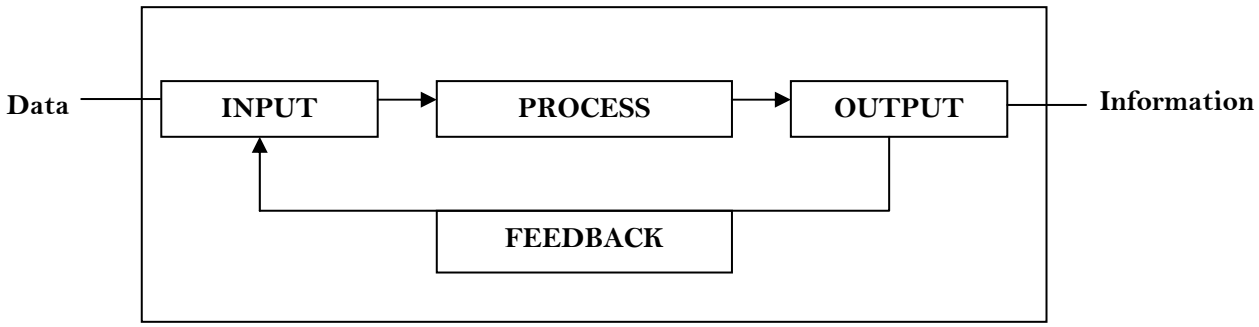
What is ICT?

ICT is the use of technology for the input of data, storage, processing to change the data into information, transfer of data to other devices and the output of information.

What is a system?

A system involves the capture of data (**INPUT**) then converting this into information (**PROCESS**) and displaying this information in some form (**OUTPUT**).

This means that all systems are based around the following model, which is the Data Cycle.



What is a system life cycle?

This is the overall process of converting data into information. 'Data' is the raw facts and 'information' is the processed data.

What is the difference between a system and an ICT system?

The difference between a system and an ICT system is that following the **PROCESS** stage the information is transferred to the people who need it or transferred into another ICT system; this is the **OUTPUT**. This output may then be used to refine the input used in the next cycle; this is known as **FEEDBACK**.

What is an ICT system composed of?

- **People**
  These can be the users of the system, or the people that maintain the system.
- **Data**
  These can be the transactions that are needed to operate the system.
- **Procedures**
  These could be the rules to safeguard the system from hackers.
- **Software**
  This could be the operating system or the application software that are required by the computer.
- **Hardware**
  This could be the workstations needed to operate the computer.
- **Information**
  This could the output of the system.

2.2 – Data and Information

This section distinguishes the difference between Data and Information. The main purpose of using ICT is to process data as efficiently as possible to produce useful information.

What is Data?

Raw facts, figures, events or transactions; these are only meaningful when put into context (e.g. 5, 12, 19 are unprocessed numbers, because they have not been put into a context).

How data can arise

There are two sources of data: **DIRECT** or **INDIRECT**:

- **Direct:** Collected for a specific purpose, e.g. buying goods in a supermarket. The bar code on the item is passed over the scanner and the data about the product is read.
- **Indirect:** Derived from data originally collected for an entirely different purpose, e.g. the data collected by the cash till is now used as data in the stock-taking program.

What form can data take?

Data can appear in different forms. It can be text (numbers and letters), numbers, sound, still or moving images.

GIGO – "Garbage In, Garbage Out"

If the data source is entered incorrectly then the information output will be incorrect.

Example:

- **Garbage In:** When entering a student's result for an exam, the teacher copies the marks for the student above him in the list by mistake.
- **Garbage Out:** As a result, the student is awarded the wrong grade.

Another form of GIGO

Example:

- **Correct data in:** The student's mark is entered correctly into the ICT system …
- **Incorrect processing:** however, there is a flaw in the program and it calculates the grade incorrectly.
- **Garbage out:** The result will be incorrect.

Encoding Data

Data for ICT systems needs to be encoded into a machine understandable format. For example:

1. Pictures into **vector graphics (e.g. jpg) or bitmapped (e.g. bmp)**.
2. Sound into **wave (e.g. wav or mp3)**.
3. Text into **documents (e.g. doc or pdf)**.
4. Movies into movie files (**e.g. mpeg**).

Coding Data

Entering data into a computer can be a slow process and as the data is entered errors can appear. Data can also take up a great deal of storage space. The data entered into most ICT systems needs to be coded so that it is reduced in size, saving computer space and reducing errors through misspelling.

Example:

M = Male, F = Female

XL = Extra Large, L= Large, M= Medium, S= Small

Examination tip: Be careful that you do not mix up coding and encoding data in examination questions.

Coded Value Judgements

Imagine a questionnaire where you are asked to tick a box rating something from 'Poor' to 'Excellent'. How much does this data really tell you? Comments or reasons really need to be included to explain answers and complete the picture. This method of data collection is only appropriate in certain areas.

Excellent	Good	Fair	Poor
☐	☐	☐	☐

What is Information?

Data that has been processed into a form that is meaningful and useful. Information is required in the day-to-day running of a business and to support decision-making. Information has context and its meaning is determined by that context (e.g. when 5, 12, 19 – a doctor's patients' ages – are entered into a spreadsheet, some functions are applied, and the names of patients and their vaccinations to date are displayed).

Factors that affect the quality of information

In addition to the points above, information is said to be of good quality if it is:

1. **Appropriate**
   Information can be produced in many forms, e.g. in a supermarket, information about the stock is produced from the EPOS system. This is then used by the people ordering new stock. However, this information will be in an inappropriate form for the manager of the store who will require far more detailed information.
2. **Clear**
   The information produced by the ICT system must be clear to read and understand. If a person has to struggle to understand the information then it is not of good quality and may not be of any use.
3. **Timely (available when needed)**
   Old information is useless. If someone was to steal an examination paper and offer it a day before an examination then it would be worth a great deal of money; a day after the examination it would be useless.
4. **Concise**
   There must be just the right amount of information displayed / stored in order for the data to be of good quality. Too much and the user will have to waste time searching for the relevant points; too little and not all the information is stored.
5. **Up-to-date**
   The information produced must be up-to-date for it to be of good quality. For example, a holiday firm produced a questionnaire in 2005 on people's holiday habits; it is planning to use the results of this questionnaire to plan holidays in 2009. The information collected is out of date and therefore useless.
6. **Correct**
   Information collected must be correct for it to be of any use.

2.3 – People and ICT systems

This section of specification looks at the reasons why ICT systems are commissioned; it also looks at the requirements and characteristics of users. The section looks at how humans interact with computers and what makes a good HCI. Finally this section looks at the qualities required for different jobs using ICT.

ICT systems are designed for and used by people and are commissioned for a purpose

When a problem has been identified by a client, the programmer produces a working solution – initially for the client, but also possibly for other users.

For example, if a client wants to produce an ordering system for his company then they would contact a programmer who would then solve the problem and create an ICT system that matches the needs of the client. This system would then be used by the client's staff.

What are the characteristics of users?

Every user of a system is different; they have different needs and need different support. Below is a list of the different requirements of users:

- **Experience**
  Users can be experts or inexperienced, therefore they will need different types of support to help them navigate around an ICT system. An expert user should have the ability to customise their software whereas an inexperienced user will need many wizards and tips to help them work.
- **Physical characteristics**
  Some users may be able-bodied whilst others have disabilities. Those with disabilities will have to have their systems adapted so that they can use them effectively. For example, some systems will require more appropriate forms of peripheral, like Braille keyboards and a larger screen for the visually impaired. This also applies to software as well as hardware.
- **Environment of use**
  The environment that the user works in will have an effect on the system that they operate. For example, a user that works on the factory floor may have peripherals that reflect this and rather than using a keyboard they will use a concept keyboard or a mouse. Users working in the catering industry are more likely to use a concept keyboard rather than a standard keyboard; this allows the user to select an object on the keyboard rather than typing in the object.
- **Task to be undertaken**
  Different systems require different tasks to be undertaken; this will affect the way that the user works.
- **Age**
  The age of the user will affect the way they solve the problem on the computer. The older a user is the more likely they are to resist change, therefore the way their system looks and operates may need to be similar to the current system. A younger user is less likely to resist change and therefore their system may be more dynamo
  ic in feel and operation.

How users interact with ICT systems

This involves the use of human computer interfaces – basically the interaction between a user and a computer. A designer aims to make a good interface so that the user does not get stressed whilst using the system. Examples of good user interface design ensure that a user can carry out their required task with the minimum amount of hassle.

A good HCI will:

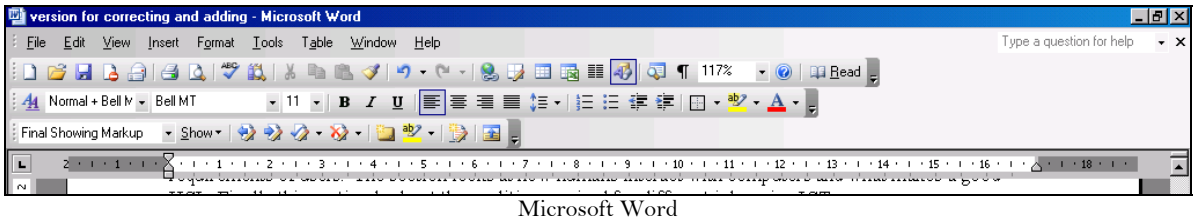
- Be easy to use for all users but specifically inexperienced users
- Be informative
- Be consistent to allow for transferable skills to be performed.
- Have facilities to customise the interface so that experienced users can use them
- Always do what the user expects
- Reduce the possibility of errors occurring
- Have help available for the user
- Take the user's health and safety into consideration

Designing a new interface
You need to consider the following:
1. Who will use the system? An IT professional or a novice user?
2. What age is the user? A child or an adult?
3. What task does the user wish to achieve?
4. Is the task repetitive?
5. Does the user require any specific knowledge?
6. Do tasks vary greatly from one occasion to the next?
7. What environment is the user operating in? Hazardous and noisy or calm and quiet?
8. What is technologically possible?

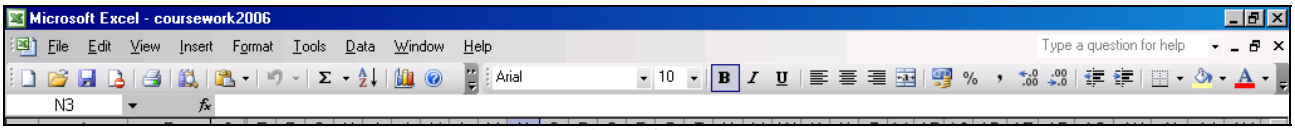
Design Tips for an effective user interface
- Don't make screens too cluttered (spaces and blanks are important).
- Items should appear in a logical sequence.
- It should be clear what needs to be entered.
- Default values, check boxes and drop down lists should be used to minimise data entry.
- The user should be given a chance to go back and correct any field before the data is accepted.
- Help facilities should be provided.
- Error messages need to be descriptive to assist the user in identifying what is wrong.
- Colour should be used carefully.

'Attention-getting' devices such as blinking cursors, high-intensity, reverse video, underlining etc. should not be over-used.

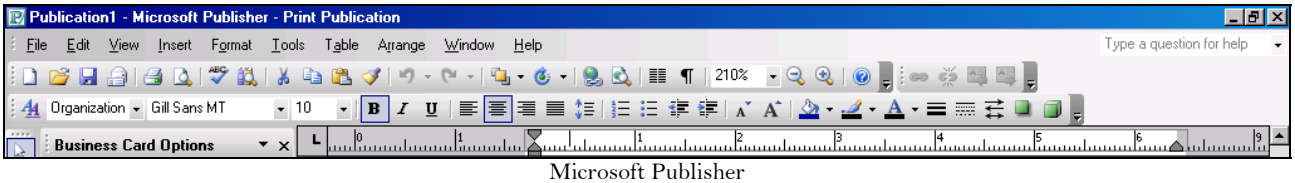
Consistency
Have you ever wondered why Microsoft products are so popular? Look at the following interfaces:



Microsoft Word



Microsoft Excel



Microsoft Publisher

Notice that the interfaces are very similar in design, the colours are similar and some of the menus are in the same place. This ensures that when one piece of software has been learnt then the skills can be transferred to other pieces of software. This cuts down on the stress of learning a new piece of software and makes use of long-term memory, so that when a brand new version of the software is produced the user will have no problem in using it.

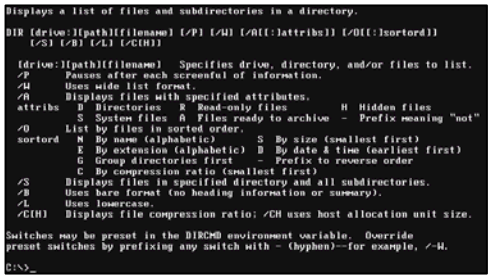
Getting help from the computer
Modern HCIs are far better in the way they give help and advice than systems in the past. The help given is context based, so that if a problem occurs whilst the user is working then the assistant (the dreaded paper clip in Microsoft products) will pop up and help you.

Asking for help on the computer now uses natural language; this is where the user types in a question to gain support in solving the problem. The result is a list of solutions that the user can choose from.

Different types of Interface

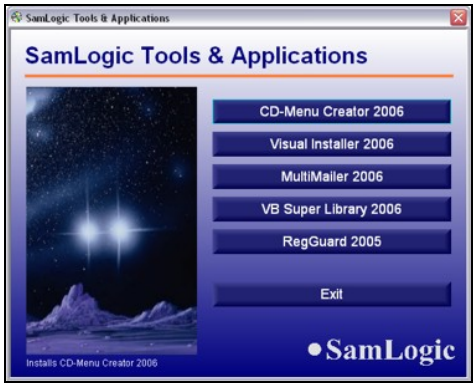
Command Line Interface

Typing in known commands to activate a program e.g. DIR for directory search in MS-DOS. This requires the user to be an expert in the use of programming, as each command must not only be learnt but also understood. Incorrectly entered commands could affect the running of the ICT system. An example of this type of interface is the setting up of the computer.



Menu Driven Interface

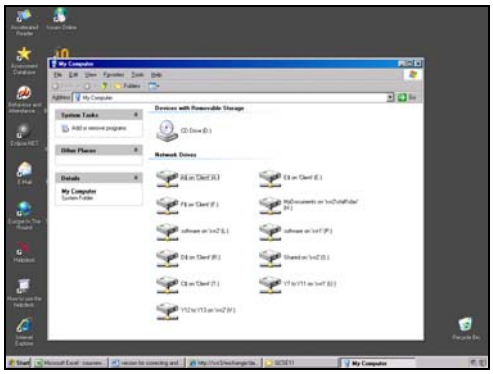
A menu driven interface is a type of interface where the user navigates through menus and sub menus in order to achieve a specific task. A use of this type of interface is in mobile phones and ipods. Many telephone call centres use this kind of interface where the user is given a series of options (menus) and has to speak or press the telephone buttons. This then leads to another menu choice or the person's directory.



Graphical User Interface

A graphical user interface allows the user to interface with the computer using icons, menus, pointing devices and other human interface devices. This is often used in PC operating systems. Systems like this tend to make use of long-term memory so that once one GUI is learnt the skills can be transferred to other software. This type of system can be used by inexperienced users and expert users as it can be customised. Its major problem, however, is that it is a massive file and if the computer system is too slow then the GUI can crash or run slowly.

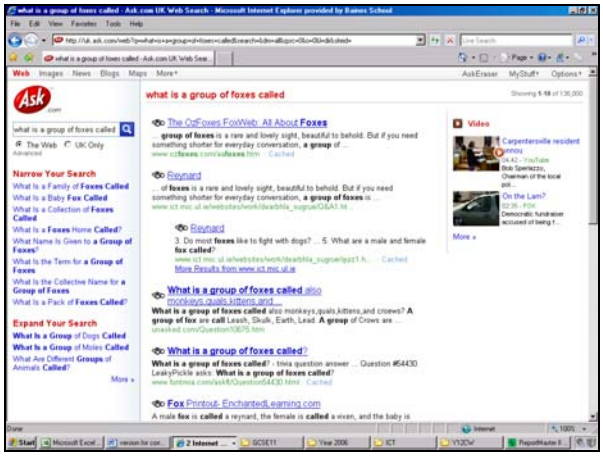
W WINDOWS **I** ICONS **M** MENU **P** POINTER



Advantages:

- Increased speed of learning, ease of use.
- Confidence building for novice users.
- Increased range of tasks solvable by inexperienced users.
- A greater range of software accessible to the average user.

Natural Language Interface
A natural language interface is one that uses commands given in spoken language or English sentences. Instead of navigating through menus, clicking on icons or typing commands, the Natural Language Interface allows a user to simply state the desired function. This can be a very fast way of operating the computer. These are sometimes used in fighter jets to allow the pilot to operate the computer without having to divert his vision to a screen or use his hands. They are also used in the National Train booking system where the user speaks to state where and when they are travelling. Internet search engines like Ask.co.uk use natural language to search for information.



Advantages:
- No need for training in a specialised command language.
- Extremely flexible and powerful.
- The user is free to construct his / her own commands.

Disadvantages:
- The need to use grammatical English.
- The need to use slang rather than 'natural language'.
- The use of natural language can easily mislead the naive user into believing the computer is much more intelligent than it actually is.

Working in ICT
For the examination students need to know the different jobs within the ICT industry. There are many available; a few of them are listed below:

Computer Programmer:
- Writes or analyses computer programs.
- Needs problem solving skills.
- Needs to be able to be patient when working with the coding.
- Needs to be able to communicate well both verbally and written.

Project Manager:
- Controls a team of professionals.
- Communicates at all levels of an organisation.
- Attention to detail needed.

Database Administrator:
- Adheres to database principals.
- Maintains databases.
- Adheres to legal requirements of storage of data.

Network Administrator:
- Needs problem solving skills.
- Needs interpersonal skills.
- Needs to understand organisations.

Website Administrator:
- Needs design skills.
- Needs communication skills.

Changes have been made to the new specification which now requires students to explain which job requires certain skills or qualities. In the past the job has been given and the qualities noted.

Qualities of an ICT Professional

- Communication and questioning skills.
- Patience to use non-jargon words.
- Calm nature.
- Good listening skills.
- Management skills.
- Analytical and problem solving skills.
- Good organisational and writing skills.
- Approachable and self-confident.
- Ability to take the initiative.
- Design skills.
- Technical competence.
- Self-motivation and initiative.
- Flexibility.

Effective teamwork
Working as part of a team is essential when working in ICT. A good team member is sensitive to the needs of other members, reliable, supportive and cooperative. Team members build on the strengths of others.

Characteristics of effective ICT teams
An effective ICT team is likely to have most of the following characteristics:

- **Good, clear and consistent leadership.**
  Each project is managed by a project manager whose job it is to direct the resources in the best possible way so that it is completed on time and to budget.
- **An appropriate balance of skills and areas of expertise amongst the members of the team.**
  Each team should include members with different skills; this means that collectively the team is stronger as it will draw on these skills.
- **Adequate planning and scheduling of tasks.**
  Planning would include: clear timescales for projects, agreed deliverables (this is the name given to what is actually produced), and agreed targets (sometimes called 'milestones'). These targets are set at the point when the client gives approval for the project to proceed.
- **Skills to monitor and control progress against the plan in order to control costs.**
  An important task for the project leader is to monitor the progress of the project and to report back to the client. The project leader must ensure that the tasks are completed on time and under budget. However, problems do arise and the team leader must take these on board, altering the schedule to ensure that the deadlines are met. Regular meetings are needed to ensure that the project is on target.
- **Adherence to agreed standards.**
  Standards are agreed formal ways of carrying out tasks. At the start of the project, standards of working need to be set and agreed on by all members of the team. If standards are used then it is easier to continue work if someone is absent and cannot carry on with their work. Standards must be adhered to and monitored throughout. Gantt charts and prototyping are examples of standards.
- **Good communication skills.**
  At least one member of the team must be able to communicate well with people outside the team in order to gather requirements and report back on progress made. Communication skills include both written and oral communication.

2.4 – Transfer of data in ICT systems

This section of the specification looks at the basic elements that form a network; the characteristics of different types of network; finally looking at standards and the appropriate and inappropriate use of networks. The specification also allows for modern technologies to be included in future examination questions, therefore you must keep up to date with emerging technologies.

It would be impossible to be successful in business today without the use of information and communication technology.

Current methods of communication

Facsimile (Fax):
- Dedicated machine or software-based.
- Recipient does not have to be there to receive document, but the machine needs to be switched on.
- Slow transmission.
- Not confidential.
- Paper copy or OCR software needed to transcribe into editable text.
- Quality of the text can be poor.
- Sending a fax costs the same as a standard telephone call.
- Faxes can only be sent to one destination at a time.

Telephone:
- Service depends upon size of bandwidth (the channel for data to pass through).
- Telephone is only for speech; time wasted in connecting.
- Telephone tag – phoning and leaving messages.
- Time zone differences affect immediate calls.
- Automated switchboards, Digital Dorothy (voice activated).
- Answer phones and voicemail.
- Mobile WAP phones and mobile systems.

EDI (Electronic Data Interchange):
- Specific transfer of data via computer systems.
- Usually for automated JIT (Just In Time) ordering systems, e.g. supermarket stock to warehouse.
- Systems must use the same standard, e.g. ASCII.

VOIP / Internet Telephones:
- Uses a PC (with microphone & speakers) to send audio in real time via the Internet.
- Much cheaper than normal phone calls (especially international calls).

More Recent Developments:
- Digital TV.
- Broadband (Cable, Modem or ADSL).
- Mobile phone, Geographic Location Device.
- GPS.
- Body sensors to detect a person's health.
- Remote communications via "hotspots".
- Bluetooth systems.

Networks

There are two types of network: Local Area Networks (LANs) and Wide Area Networks (WANs). Local area networks are located in a building or on a site and are usually hard wired, whereas WANS are linked across countries and continents and are usually communication networks.

A number of different devices are used to set up a network or to link two networks together. Each computer on the network needs a network interface card (NIC) and a cable or a wireless connection. This allows it to link to other computers and devices. Networks usually have a file server where all the data and possibly programmes are stored. If the network is to connect to a WAN then a modem will need to be used to translate the binary signals of the computer to the analogue signals of the telephone systems. Modems are also used on broadband systems even though the communication system is binary. Other ways of linking two networks are:

Bridge: used to link two similar LANS
Gateway or router: used to link two different networks e.g. LAN and a WAN
Repeater: used to boost the signal of a LAN

A network also needs software in order to operate properly. The software used to manage and control the network is the network operating system and this is housed in the server. Each computer will need an operating system, and if the network is connected to the Internet or an intranet, will need a browser. Email software will be needed so that the communication across the network can be achieved. As the network is connected to the Internet or other networks a firewall will be needed.

Finally there have to be some rules for transferring the data across the networks; these are communication protocols. The rules need to be set so that data that is set by one computer system can be easily read by another. For example, TCP/IP is the set of rules that allow data to be split into packets and sent across the Internet.

Advantages of a LAN:

1. Sharing of disk storage, printers, modems, scanners, etc. and possibly central servers.
2. Sharing of data held on disk drives accessible by all users.
3. Sharing of software.
4. It is easy to upgrade software and set up new users as it is centralised.
5. Ability to communicate with other users on the network.
6. Centrally controlled security both in terms of access to and backup of data.
7. No need for duplication of data; one central copy can be maintained.

Disadvantages of a LAN:

1. If the central file server fails, network users cannot work.
2. If part of the network goes down, some resources may not be available.
3. Hackers have access to an entire network of PCs as opposed to one stand-alone machine.
4. Viruses can spread easily around a network.
5. As the traffic increases on the network, the performance may degrade.
6. Dependency on systems manager / administrator to provide service.
7. Little local control over your own machine, what is installed and what you have access to.
8. Start up costs are expensive due to the purchase of other equipment.
9. Reliant on other users not hogging resources, e.g. printing out very large documents during busy office hours causing a bottleneck of print jobs.

Types of LAN

Client Server Network

- Central storage and sharing of programs and data.
- User IDs, passwords and access levels are controlled centrally.
- Central backup.
- Communication takes place through the server; if the server goes down all users are affected.
- Can be used for networks of any size.
- Client devices send requests for service and data, such as printing or retrieval of data to a specific server that then performs the processing.
- Computers may be of different types.

Peer-to-Peer Network – *max 15 computers*

- Distributed storage, software held on machines individually.
- Security is set on each machine.
- Backup is the responsibility of each user.
- No central reliance.
- All computers control their own communication.
- Typically only used for smaller networks.
- Each workstation can communicate directly with every other workstation on the network without going through a server.
- Computers must be of the same specification

Components of a LAN

1. Workstations – PCs or terminals.
2. A server (which could include a file server, a communication server, etc.) - a special PC or larger computer where shared software resources are stored, including the network software that monitors network operation.
3. Cabling – to link the computers together.
4. Network cards, which have to be inserted into each computer on the network to give it a unique identity and allow it to interact with other components of the network.
5. A print server controlling access to network printers ensures these resources are shared equally between users and manages print queues.
6. Some form of backup facility. Some LANs have two file servers, with data being copied from one server to the other at regular intervals so that if one goes down, the other can take over with the loss of only a few minutes work.

The Role of a Network Administrator

- Installing and upgrading hardware and software when necessary.
- Adding new user profiles.
- Maintaining access rights / levels.
- Keeping users informed of changes.
- Backups.
- Disaster recovery.
- Troubleshooting network problems.
- Virus protection.
- Ensuring network security is maintained.
- Monitoring the network to ensure response times are adequate.

Wide Area Networks (WAN)

A collection of computers spread over a wide geographical area; may make use of microwaves, satellites or telephone lines. There are two main types of telephone lines utilised:

- **Public lines**, on which the cost of sending data depends on the length of time taken.
- **Private or leased lines**, for which there is a fixed annual fee and the line can be used as often as needed for no extra cost.

Communications Media

Communication can take place over a combination of different media:

- **Twisted Pair** (Copper Wire) – used in much of the telephone network.
- **Coaxial Cable** – high quality, well-insulated cable, transmits data at fast rate.
- **Fibre Optic** – uses light pulses, fast transfer of data.
- **Microwave** – travels over long distances. Used for mobile phones.
- **Satellites** – travels over long distances. Used for mobile phones.

Methods of Data Transmission

- **Asynchronous:** Sends one character at a time with each character preceded by a start bit and followed by a stop bit. A **Parity bit** is also usually included to combat incorrect transmission of data.
- **Synchronous:** Timed transmission, no need for starts and stop bits. Used by mainframe computers and is less prone to error.

Factors affecting rate of Data Transmission

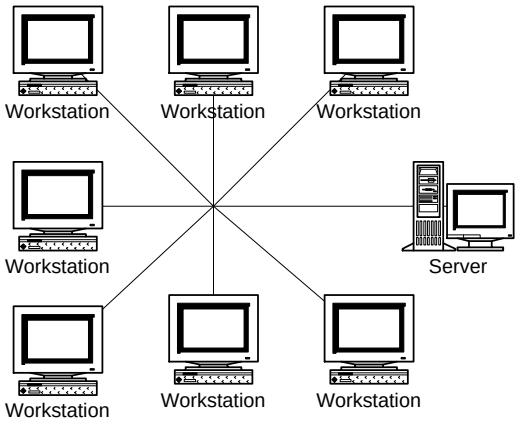
- The speed of the modem.
- The nature of the transmission line; a digital line such as an ISDN line has a much higher transmission speed than an analogue line.
- The type of cable used: twisted pair has a transfer rate of 10mbps; fibre optic cable is about 10 times as fast.
- The type of transmission: synchronous or asynchronous.

Examples of Network Topologies

The topology of a network is its physical layout; the way in which the computers and other units are connected.

Star Network

Each node in a star network is connected to a central computer that controls the network. Network signals travel from the server to the station along each individual station's cable. A polling system is commonly used where the file server polls each station in turn to see if it has a signal to send. The server then handles signals as they are received.



Advantages:

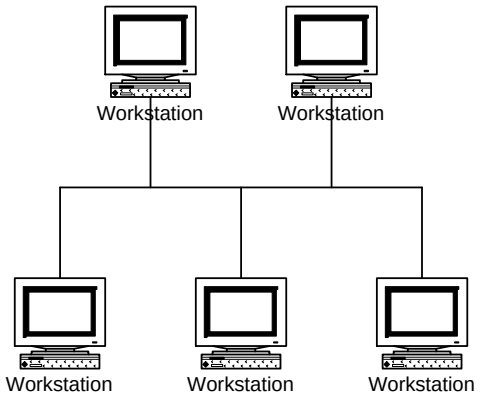
- If one cable fails, the other stations are not affected.
- Consistent performance even when the network is being heavily used.
- No problems with 'collisions' of data since each station have its own cable to the server.
- Easy to add new stations without disrupting the network.

Disadvantages:

- May be costly to install because of the length of cable required.
- Reliance on central host.

Bus Network

In a bus network, all the devices share a single cable. Information can be transmitted in either direction from any PC to any other. Several stations may want to transmit down the same line simultaneously, and there has to be some strategy for deciding who gets the line. Ethernet uses a collision system; before a station begins transmitting, it checks that the channel is not busy; if it is, it has to wait before transmission can begin. Once transmitting, it listens for other nodes also beginning transmission. If the transmitted message collides with another, both stations abort and wait before trying again.



Advantages:

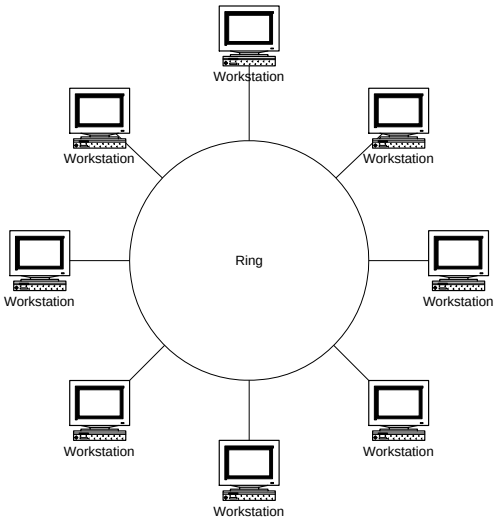
- Easy and inexpensive to install as it requires the least amount of cable.
- Easy to add more stations without disrupting the network.

Disadvantages:

- The whole network goes down, if the main cable fails at any point.
- Cable failure is difficult to isolate.
- Network performance degrades under a heavy load.

Ring Network

In a ring network, a series of computers are connected together and there is no central controlling computer. Each computer may communicate with any other computer in the ring, with messages being specifically addressed to the destination computer.



Advantages:

- There is no dependence on a central computer or file server, and each node controls transmission to and from itself.
- Transmission of messages around the ring is relatively simple, with messages travelling in one direction only.
- Very high transmission rates are possible.

Disadvantage:

- If one node in the ring breaks down, transmission between any of the devices in the ring is disrupted.

The Internet (International Network):

A worldwide network made up of Local Area Networks (LANs) and Wide Area Networks (WANs). It has no central governing body and there is no control of content. It continues to grow at a phenomenal rate. There are approximately 17 billion websites on the Internet. Millions of users are accessing the Internet at any one time.

Accessing the Internet

What is required to access the Internet?

1. An ICT device (this could be a computer, a mobile phone, etc.).
2. A Telephone Line (standard, ISDN, ADSL) or a wireless connection.
3. A Modem (Modulator / Demodulator) for analogue lines to convert computer signals.
4. Connection via an ISP (Internet Service Provider).
5. An Internet Browser software, to display web pages in human form (HTML).

Online Services provided by the Internet

There are many different types of Information Services offered on the Internet, divided into 'Information-Based' and 'Service-Based' provision.

Information-Based

- News
- Share prices
- Weather
- Sport
- Bulletin boards/forums (allow people with the same interests to swap ideas)

Service-Based

- Banking
- Shopping
- Education
- Entertainment (music and games can be downloaded)
- Software help and support
- Job hunting

Email

Email is fast replacing the traditional postal service, now known as 'snail mail'. Email has now become the main way of communicating person to person as it allows attachments and messages to be sent at any time to a known email address. The main differences between email and its main rivals, i.e. the telephone and the post, are that with the telephone there is no permanent record of the message, and unlike postal mail, email allows multiple copies to be sent at once very easily. One big drawback of email compared with postal mail is as follows:

Postal address – correct
Mr A Smith 1 The Cottage High St Blackpool FY1 8BE
Email address – correct
Smith.a@blackpool.co.uk

Postal Address – incorrect
Mr A Smith The Cottage High St Blackpool FY1 8BE
Email address – incorrect
Smith.a@blacpool.co.uk

Post being sent to the incorrect address will be delivered even with parts of the address missing. However, an email being sent to the incorrect email address will not get delivered, as the address has to be perfect. Therefore there is more chance of messages being lost via email than in the post.

Advantages of Email:

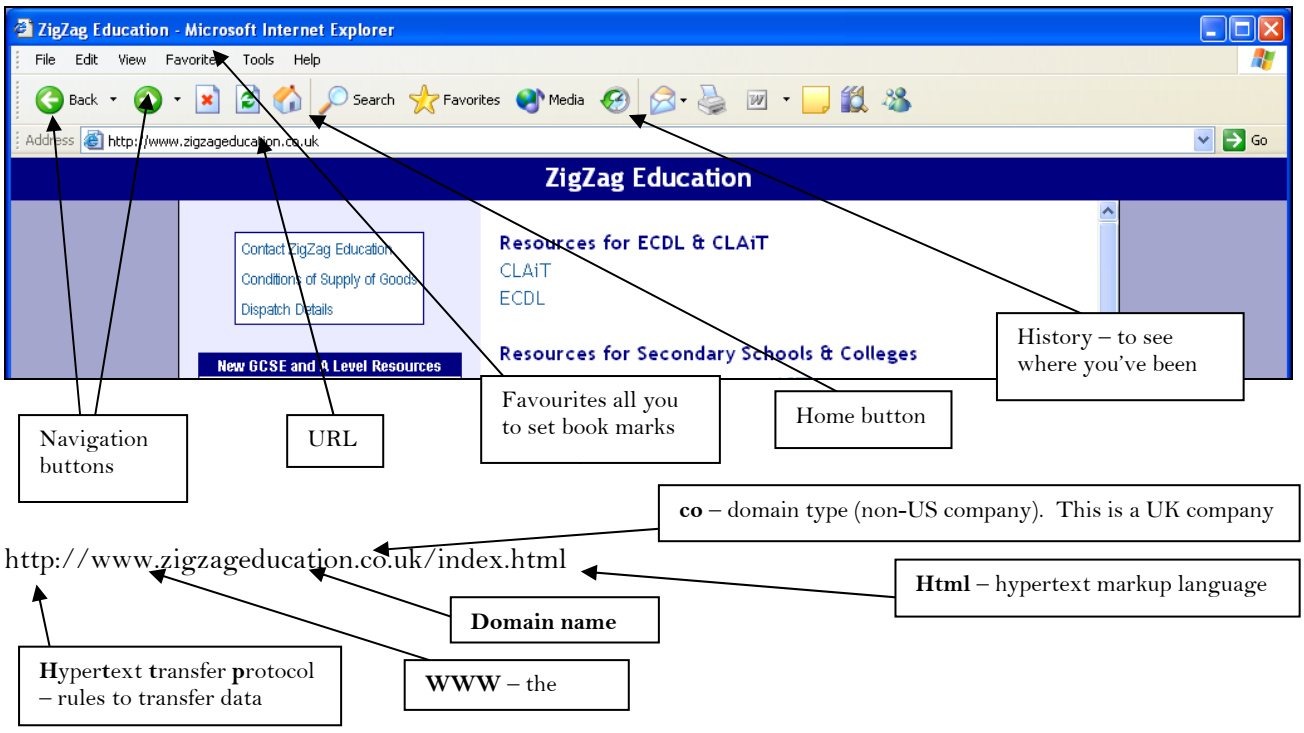
- Message sent almost instantaneously.
- Easy / convenient to send and receive information.
- Allows attachments to be sent and received and these are in digital form.
- Same message can be sent simultaneously to a number of people.
- Can confirm delivery and / or that the mail has been read.

Matters to consider when using the Internet:

- Security of data
- Viruses
- Hackers
- Espionage
- Employees wasting work time

The World Wide Web (WWW)
The World Wide Web is only part of the Internet, which also includes Gopher, newsgroups, email and other areas. The Web is a collection of web pages stored on computers throughout the world, joined by hypertext links. A link may be text or graphics; when you click on a link you are taken automatically to a related web page or another resource like a sound file or a movie. Access is provided and facilitated by browsers such as Netscape or Internet Explorer. The creation of the Web is attributed to Tim Berners-Lee in 1989 who invented an easy way to use browser software.

Use of browser software



An intranet
This is like a 'private internet' for an organisation to communicate within itself, therefore not accessible to the outside world. The intranet is a network of computers that allow sharing of information in a user-friendly fashion.

An extranet
This is a collection of a number of intranets and is spread over the whole of a company with the intranets being the branches, for example. An extranet allows a user access to the other intranets it contains as well as the Internet. This allows for communication within and outside the company.

Teleconferencing
A communication system that allows people in different physical locations to exchange ideas and information interactively with the use of internet technology; sometimes this is known as a conference call.

A number of people in different locations around the world can have a multi-way conversation via internet technology. Some public telephone systems like BT have the facility to set this up or it can be done by all the participants dialling in to a central conference call number.

Video Conferencing
This is a part of teleconferencing but carried out with the use of video cameras, microphones, large monitors and computers. It requires a *'high-bandwidth'* (at least ISDN) communication link. *Bandwidth* is a measure of how much data can be passed down a line. It allows people in different locations to hold an interactive, real-time discussion and to actually see each other while doing so.

Teleconferences can be carried out at short notice so that the user does not need to travel to a common meeting. This saves the cost of conference facilities, cost of travel and the time taken to travel. There are, however, limitations with using this equipment; firstly the massive cost of a professional unit, somewhere in the region of £60,000; then there is the speed of connection. Video slows down the connection, therefore if the connection speed is slow, the video will not work. Many companies opt for teleconferencing rather than video conferencing. Teleconferencing slows down communication, therefore after a few sessions a main meeting is needed.

2.5 – Safety and security of data in ICT systems

This section looks at the need to protect data in ICT systems and the subsequent threats if these measures fail. It also looks at the physical protection of ICT systems and the legislation that covers the safety and security of data.

Threats to ICT systems

As ICT has developed, computer crime has increased. Here are a number of threats that can be suffered by ICT systems, many come from the Internet:

- Fraudulent traders
- Paedophiles
- Hackers and crackers
- Software pirates
- Terrorists
- Money & personality theft
- Music and moving images pirates
- Organised criminals
- Organised hooliganism
- Viruses
- Publishing inaccurate, libellous information
- Identity theft
- Blackmailing and stalking
- Natural disasters

Internal Threats to ICT Systems:

- Hardware failure
- Faulty procedures
- Poorly-trained staff
- Use of laptops
- Dishonest employees

Any unauthorised access to computer data is illegal. Data that has been accessed can be altered, copied and then removed from the system, or deleted. Viruses can be sent to people and companies, although it is not against the law to create a virus. The reason for this is that software companies have to produce viruses to understand how they work so that they can develop anti-virus software.

Hacking

Unauthorised access to data held on an ICT system, from internal or external personnel. This appears in two forms: the first is simply an employee or person who gains access to an ICT system to look at the data but not to change it; the other is to gain access to an ICT system and then change the data in some way. This is often carried out by corrupt employees or employees with a grudge as they have insider knowledge of passwords and user IDs. The motive for doing this ranges from employees' boredom to espionage and stealing commercial material from another company.

Fraud and transfer of funds illegally

Fraud is the act of deliberate deception with the intention of gaining some benefit. Money does not technically exist now unless you hold it in your hand; when you go shopping and pay by card, no money physically changes hands, but it is electronically transferred from your account to the shops account. This is a legal transaction but a criminal could do exactly the same thing illegally by transferring money from someone else's account into their own.

Internet fraud is a similar offence but this time it is subtly produced. A criminal sets up a fraudulent site claiming to be a particular organisation, offering goods for sale. Unsuspecting customers buy the products which are never delivered although the money is transferred to the criminal. The criminal may then have the credit card number and details so they can make further use of the card. Many of these sites are pornographic, therefore the owners of the cards are not too happy about admitting that they have been the victim of fraud. This continues to be a problem as the Internet is not policed. The setting up of illegal financial websites or sending emails stating that they have come from a legitimate financial site is called 'phishing'.

Software and music piracy
As with money, the way we purchase music and software has changed. We no longer tend to go into a shop and buy these products; we download them from the Internet. This in most cases is legal, however, as with the transfer of funds, people can visit illegal music sites and download the music illegally or even download a legal copy then distribute it to others. This is costing the music industry millions of pounds. Similarly criminals can film a new movie in the cinema using an electronic device then upload this to the Internet for others to purchase, again costing the movie industry millions of pounds in lost revenue.

Protecting the data on the Internet

Secure Website Indicators include:
- A URL that starts with 'https' (uses the encryption protocol - SSL (Secure Socket Layer)).
- The padlock logo in the task bar on the site indicates that it is a reputable / secure website; this means that any transactions are encrypted and therefore safe.

Malpractice and Crime
Not all incidences of data lost from ICT systems are a result of illegal practices. There is the problem of malpractice (which means bad practice). For example, an employee who cannot remember their password and who decides to use a Post-it note fastened to their computer screen acts in an unprofessional way. They are leaving their computer station open to hackers. This may sound silly, but I observed it in an office by an open hatch, so that anyone could see the password. Another form of malpractice is to allow employees access to CD drives or USB pens so they can bring in software from home, this software will be unchecked and therefore may carry a virus. Malpractice is acting in an unprofessional way; it is not against the law but is against the laws set by the company.

Computer crime is against the law; this means if you commit computer crime then you break the law of the land and therefore pay the consequences. For example hacking in to an ICT system or introducing a virus.

Protecting ICT systems
Data and programs are vulnerable to both deliberate and accidental damage ranging from something as minor as a CD-ROM that becomes unusable, to hackers stealing millions through a network link from a major organisation.

Measures to Protect ICT Systems from Threats:
Most companies have strict procedures in place so that the sensitive data they hold is protected; these can include:
1. Physical restrictions; swipe cards, servers in locked room / box.
2. User names and passwords; must be a combination of characters and digits.
3. User groups and access privileges.
4. Audit trail software.
5. Data scrambling using encryption.
6. Backup.
7. Careful vetting of staff.
8. Training staff.
9. Installing virus checkers.
10. Installing a firewall.
11. Levels of access.
12. Uninterrupted power supply.
13. Internet filters.

Viruses

A program or file that can destroy or damage a computer system and has the ability to replicate itself. Viruses occur while transferring data from computer to computer via portable storage devices, email, or while downloading files from the Internet.

Limiting the risk of Viruses

- Do not load any unauthorised software onto a machine.
- Do not download any software from the Internet.
- Do not insert a portable storage device from an unknown source or open an unknown email.
- Install and run virus checking software.
- 1,000 viruses are created a week, keep the virus checking software up to date

Internet Access Issues

Schools must guard against pupils accessing pornographic materials and participation in chat rooms where pupils may be exposed to undesirable strangers.

Businesses may want to control use of email and Internet to business use only. Some organisations achieve this by installing and maintaining their own **intranet** (private internet) and / or they have a **firewall** to prevent unsuitable material being downloaded.

Security, Privacy and Integrity

- **Privacy** – the data can only be accessed by and disclosed to authorised persons.
- **Integrity** – correctness of data during and after processing.
- **Security** – protecting the ICT system from attack.

Levels of Access to Data

Users of a network are often supplied with a **Username** and **Password**. The Username gives access to the computer system whereas the Password protects the user's area. Together they form the security of the system. Different users have different access rights to the network; some are given simple access to an area but others, like the network manager, will have full access. As well as this, within most commonly used software, data permission levels can be set.

The most common levels include:

1. No Access.
2. Read Only.
3. Read and Amend.
4. Read, Amend and Delete.
5. Full Access.

Some systems only allow users to access either the system or certain types of software at certain times of the day. Others only allow users to operate certain computers on the network for certain types of application.

Remote access normally involves pre-specified telephone numbers. For example, on receipt of a call from a remote user, the host computer will automatically call back on a pre-arranged telephone number before allowing log on. This is known as **dial-back/call-back**.

Biometric Methods

Using biological features previously recorded onto an embedded computer or chip, to identify users:

- Fingerprint Recognition
- Voice Recognition
- Face Recognition
- Iris Recognition
- Infra-red scans to examine pattern of blood vessels

Legislation

Computer Misuse Act, 1990

The act was introduced in order to cover a host of computer crimes that are not covered in existing laws.

What the Law consists of:

- Deliberately planting a virus in a computer with the intention to cause damage.
- Using computers in work time to carry out unauthorised work.
- Copying computer programmes illegally.
- Hacking into someone else's system to view or change information.
- Using computers for fraud, e.g. fictitious employees on payroll.

Official Categories:

- **Level 1:** Unauthorised access to computer material. For example:
  - Breaking the password code into the Bank of England to brag to your mates.
  - Downloading software illegally.

  Penalty: maximum 6 months in jail and / or a £5000 fine.

- **Level 2:** Unauthorised access with intent to cause a further offence. For example:
  - Fraud.
  - Blackmail.

  Penalty: maximum 5 years in jail, plus a fine.

- **Level 3:** Unauthorised changing or deleting of files. For example:
  - Intentionally introducing a virus.

  Penalty: maximum 5 years in jail, plus a fine.

The Consequences:

On looking at whether an offence under this act has taken place, it is necessary to prove intent.
The court then has to prove that the person who did the act intended to gain access to data and programs, didn't have the authorisation to do so, and knew and understood that they didn't have authorisation.
Very few cases under the act have ever come to court.

Problems with the Act

One bizarre loophole in the act under level 3 is that an employee could have broken the act by uploading loads of large files on to a work computer so that it slowed the performance of the computer.

The main problem with the Computer Misuse Act is that it came into force before the full introduction of the Internet and therefore does not cover all the problems that are now associated with the Internet.

Data Protection Act, 1998

- By 2007 this act will cover manually held data as well as computer records.
- This act of Parliament protects data and the privacy of the person the data is about.

Data Subjects:

The living individuals who have personal data held about them on an ICT system. The Data Protection Act allows individuals to have access to information held about them on a computer and where appropriate to have it corrected or deleted. A data subject does not need to give permission for data to be held about them; only if the data is sensitive does permission need to be sought. Sometimes consent is implicit, i.e. filling in a form, and anything pertaining to law, justice, and government does not need permission.

The Rights of Data Subjects

- The right to compensation for unauthorised disclosure of data.
- The right to compensation for inaccurate data.
- The right to compensation for unauthorised access, loss or destruction of data.
- The right to access the data held about them and to have it rectified or deleted, if inaccurate.

When can personal data be processed?
Personal data can be processed if one or more of the following conditions have been met:
- The data subject has given their consent.
- It is a legal obligation.
- It is necessary to protect an individual's vital interests.
- It is necessary for the administration of justice.

Information that must be provided by the data user about the data that is to be stored:
- Description of purpose(s) that data is to be stored for.
- Type of data to be stored.
- Who will have access to the data (recipients).
- Any organisations to which data will be passed on (data transfers).
- Sources of data or how the data has been acquired.

Who are Data Controllers?
Data controllers are those who control the contents and use of a collection of personal data and liaise with the data subjects. All data controllers have to register:
- Their name and address.
- A description of the data subjects and why data about them is being held.
- The data being held and how they intend to use it.
- A description of sources from which the data is obtained.
- A description of the persons to whom it is intended to disclose data.
- Any overseas countries to which data may be transferred to.

Who is the Information Commissioner?
This is an independent official, appointed by the Crown, to oversee the Data Protection Act 1998 and the Freedom of Information Act 2000 and to report back to Parliament.

The Commissioner's responsibilities include:
- Being responsible for making sure that the Data Protection Act is enforced and that all data controllers comply with it.
- Give advice on issues relating to the act.
- Give examples of good practice and consider complaints from data subjects.
- Ensure that the Freedom of Information Act 2000 is enforced.

The Data Protection Registrar
- Administers a Public Register of all Data Controllers.
- Promotes compliance with the Data Protection Principles.
- Investigates complaints and initiates prosecutions for breaches of the act.
- Provide guidelines for data users and subjects.

The 8 principles of the Data Protection Act:
1. Data shall be processed fairly and lawfully.
2. Data shall be obtained only for one of more specific purposes and must not be processed in any other way.
3. Data shall be adequate, relevant and not excessive in relation to the purpose.
4. Data shall be accurate and where necessary up-to-date.
5. Data should not be kept longer than necessary for the registered purpose.
6. Data shall be processed in accordance with the rights of the data subject.
7. Data shall be held securely.
8. Data shall not be transferred to a country or territory outside of the EU unless there is adequate data protection legislation in operation.

Who is exempt from the Data Protection Act?
Parts of:
- Payroll, pensions, tax and accounts data.
- Data used for household and recreational use (in some cases).
- Statistical or research purposes, e.g. census.
- Crime and National Security.
- News archives, literature and art.
- Person's household and family data.
- Mailing lists as long as name and address only.

Problems with holding data
Everyone has the right to see data held about them, or do they? They can do this by visiting the place in person, giving proof of identity or writing to the place where the data is held or telephoning and asking to see the data. This may carry an administration fee. Once the data subject has viewed the data they can ask for it to be changed if the data is incorrect or claim compensation if the error caused loss or distress.

However, not all data held about a person can be viewed. Data that could affect a criminal investigation or the outcome of a court case or even identify another person, who has not given consent, would all be exempted from subject access.

The Criminal Records Bureaux have access to criminal records; they need access to these to check out people for particular jobs, like teachers for example. People give permission to this sensitive data through a disclosure, but there are potential problems, for example:

- Getting the wrong person, due to the same name.
- Linking people through addresses, even though they did not live in the house at the same time.
- Identifying other people who have not given consent.
- Accessing data that is exempted from subject access.
- Only where the person has been caught and convicted is the data held, so crimes under investigation slip through the net.

A major consequence of this was in the Soham murder case where Ian Huntley, the murderer, had been investigated for a similar crime but had been found 'not guilty'. This was not on his record, so the CRB did not know of this when he was investigated for the caretaking job in the school.

Copyright, Designs and Patent Act, 1988

The Copyright Designs and Patents Act 1988 covers a wide range of data files such as music, literature and software. The copying of files without the permission of the owner or copyright holder make it illegal to:

1. Copy software.
2. Install pirated software(s).
3. Transmit software(s) over a telecommunications line, thereby creating a copy.
4. Software licensing.
5. Use software without a proper licence.

What is a Software Licence?
This refers to an individual who only owns a licence to use a piece of software - not the software itself.

Typical types of Software Licence are:

- **Single User** –The user is allowed to install the software on a single machine. Sometimes this will be extended to allow the user to install the software on several machines as long as, at any one time, only one of the copies is in use.
- **Multi-user** – Companies use this to purchase software for many computers. They specify the number of users that can use the software at any one particular time as opposed to the number of machines. This is for software that is not networked.
- **Network** – A Network Licence allows the software to be run on a number of machines on a local network. Normally the maximum number of machines will be stated in the licence.
- **Site** – A Site Licence allows the user to install the software on all machines - whether or not they are networked.

As with the Computer Misuse Act, this act of Parliament was introduced before the Internet was in full operation, although much of the activities of the Internet are covered in the act. Changes, however, will need to be made soon to block all loopholes.

Freedom of Information Act 2000

This act sets the rules on access to information or records held by government bodies. In general, such laws define a legal process by which government information is required to be available to the public. In many countries there are constitutional guarantees for the right of access to information, but usually these are unused if specific legislation to support them does not exist. The UK has privacy and data protection laws in operation and these form a part of the Freedom of Information Act

Telecommunications Act 1996 & Telecommunication (fraud) Act 1997

This act of parliament covers the general duties of telecommunication carriers which include telephone and wireless companies. It grants the licenses for broadcasting companies to broadcast television, digital television, satellite, cable, automated ship distress and air safety systems and radio.

The act also regulates the scrambling of television services so that obscene programmes are not broadcast. This part of the act can overlap onto the communication of obscene material to and from a computer.

In 1997 an extra section was added to make it an offence to carry out fraud from online shopping. Prior to this date the laws covering fraud did not include telecommunication links and therefore fraud was legal on the Internet.

2.6 – Backup and recovery

Backups

It is important for any company or organisation to have a tried and tested, effective backup in place and that this is carried out regularly. Depending upon the data being saved and the uses of the ICT system, you would have to consider the best method of backup to use. The backup and subsequent recovery is dependent upon:

1. What to back up?
2. How often?
3. What medium to use?
4. Where to store the backups?
5. Who will carry out the backups and the recovery?
6. What recovery procedures are in place?
7. How long should you keep backups for?

Backups need to be regular enough so that if the whole system was lost, and restoration took place, the data would still be of use. The type of backup that is carried out will depend on how frequently the data is changed. Backups tend to be carried out at night when the system is not in operation and the files are closed. Passworded files are not backed up. Backups tend to be stored off site, usually with a manager, although some backups are stored in fireproof safes, above flood level within the company. It is important that all backups are verified and tested so that they can be restored.

Types of Backup

Periodic Backups:
The most common method where all files are copied regularly (e.g. weekly) and kept in a safe place; For example stored off-site in a fireproof safe.

Incremental Backup:
When huge quantities of data are involved, backup can be reduced by only backing up those files that have changed since the last backup. This could be a daily backup.

Online Backups:
These are especially common for database systems, transaction processing systems or real time systems, where the system does not shut down.

Transaction Logging
Information about every transaction (change to the database) is recorded on a separate transaction file. If the system fails, the database can be restored from the previous night's backup and then updated from the transaction file to reflect the position immediately before the failure.

RAID
Short for Redundant Array of Inexpensive Disks where two or more hard drives are used in combination for fault tolerance. There are different types of RAID available:

- **Disk Mirroring:** Data is written to two duplicate disks simultaneously. This way if one of the disk drives fails, the system can instantly switch to the other disk without any loss of data or service.
- **Data Striping:** (Spreading out blocks of each file across multiple disks), reserving one dedicated disk for error correction data.

This and DAT – Backup Media

The type of media that you store the backup on is very important; for example, you would not try to store the day's accounting on a floppy disc, although a school I worked at did just that for 5 years. Well they *thought* they did. In reality, the data was not checked and the backup had not been made.

Below are some examples of backup media:

- Floppy disc – many devices do not now include a floppy disc drive. The capacity of the disc is small and is only useful for saving a few files.
- Memory stick – this is replacing the floppy disc as it has the added advantage of memory capacity. A full backup from a home computer can be stored on the device. It is easy to use and is easily portable.
- CD-R and CD-RW – These devices store about 700 Mb and are reasonably cheap and portable.
- MP3 players – these devices are portable and have a storage area which could be used in an emergency for storing a backup of files.
- DVD-RAM – like the CD version this is reasonably cheap although it can store 4.7Gb
- DAT – this is the modern version of the music cassette although it is smaller and stores far more data. These are used in commercial organisations to store backups. The problem with these types of devices is that they are serial, which means you have to track through all the tape to gain access to the data required.

- Removable cartridge devices – these connect via the USB port and save about 90Gb of data. An example of this is the Iomega REV.
- AIT – Artificial Intelligent Tape. This is similar to the DAT but it contains a chip which houses a catalogue of the data stored and therefore speeds up restoration of data.
- External Hard Drives – this is an extra hard drive that connects to the computer, often using a USB port. This is a portable device.
- Mirroring devices – data is constantly being written to this second hard drive, so a second copy is always available.

2.7 – What ICT can provide

What ICT can provide?

- **Fast, repetitive processing.**
  Weather forecasting systems use a special type of computer called a supercomputer designed to carry out fast, repetitive processing, sometimes called 'number crunching'. Similar systems for producing utility bills carry out processes like calculations in order to produce an accurate bill. Robots, designed to create cars, carry out fast, repetitive processing so that the cars produced are all the same and built to the same standard. Therefore these processes are carried out time and time again without making mistakes.
- **Vast storage capability.**
  Most industrial ICT systems are designed to store vast amounts of data. As computers are now used more and more for systems like the census, shopping online, and online databases (such as the one held by the DVLA), they are required to store a massive amount of data. For example, the census stores at least 58 million records.
- **The facility to search and combine data in many different ways that would otherwise be impossible.**
  As stated previously, a computer stores massive amounts of data; this data needs to be retrieved quickly for it to be useful. The Internet is a vast database which has to be searched quickly in order to be effective, for example if you search for the word 'computer' on Google, it will search 114,000,000 websites in 0.1 seconds; this would be impossible to do any other way. When the data is retrieved it can be merged with other items to produce things like invoices, mail-merged letters etc.
- **Improved presentation of information.**
  When a computer is used the output looks far more professional than the same work could be if carried out by hand. If, when the presentation has been produced, it does not match the needs of the client then it can be easily changed without having to produce the whole thing again.
- **Improved accessibility to information and services.**
  With a vast amount of data stored it is necessary that any information is easily accessible through searching and layout. This can be achieved easily through the use of ICT.
- **Improved security of data and processes.**
  Files that are not stored on a computer can be locked in a filing cabinet, but if someone gains access to the filing cabinet then these files become vulnerable; on a computer system each file can be encrypted so the data contained is scrambled and then protected with a password. This means that any data is far more secure on an ICT system than stored manually.

Is the use of ICT systems always appropriate?

- ICT systems have limitations in what they can be used for
- ICT systems have limitations in the information that they produce
- ICT systems do not always provide the most appropriate solutions

ICT systems improve the way that we process data and make life easier for the operators and help to make work more efficient; however, sometimes even a computer can get it wrong. The three main reasons for this are hardware, software and the inability to transfer data properly from one system to another.

A computer can store a large volume of data, but if you do not have the space to store this data then the computer can stop working or freeze. Processing large amounts of data can eat into processing space and processing time; if the computer does not operate fast enough the processing cannot be carried out efficiently. If your computer crashes then you could lose all your work, if this computer is a server or a main computer in a company then a great deal of people will be affected.

If software is badly written or not tested before it is released to the general public then it will not operate as it is supposed to do. If there are bugs in the coding then this could cause the system to crash. If the software is not tested properly then this could lead to embarrassing errors.

Why do ICT systems fail?

The larger the system, the more severe the consequences if a system fails. For example, the failure of the Traffic Lights Control Centre or the Airport Flight Control Centre could have truly devastating consequences.

Reasons for Failure:

- Bugs in the software.
- Implementing system too quickly.
- Requirements of the organisation are not met.
- Insufficient testing.
- No end-user involvement.
- Cutting costs with employees.
- Insufficient hardware.
- New system is not compatible with the old system.

Different types of computer or even different types of operating system store their data differently, so data sent from one type of computer to another – for example from an Apple Mac to a PC – may not be understood. Companies have tried to get round this problem by creating systems that emulate other systems or save data in a common format like RTF (Rich Text Format) or PDF (Portable Document Format). The Internet is the big success story of this transfer of data in that WebPages can be viewed on any computer, irrespective of operating system or type, as they use a common format and programming language.

Types of processing

Batch processing
This is the simplest of the processing systems and is not time dependent. Large volumes of similar transactions are collected over a period of time, then these batches are processed together, usually at night when the ICT system is quiet. The data is out of date very quickly and therefore used for billing systems where this is not critical. The operation is automatic, therefore if there is a problem there is no one present to sort it out.

Used for the production of bank statements, credit card statements, payroll, and utility bills like telephone, gas, etc.

Interactive processing
This allows the user to communicate with the computer. This requires the user reacting to the output of the system and then entering more data. The system operates quickly so that the user can keep reacting to the system.

Used in touch screen booking systems, cash machines or kitchen design.

Transaction processing
This is sometimes called pseudo real-time processing and deals with e-commerce. Data for each transaction is entered at source and processed immediately. Each transaction is completed before the next one is started. In booking systems where this is used this stops double booking, as the transaction is locked until it is completed.

Used in booking systems.

Real Time processing
This system will react fast enough to influence events outside the ICT system. This system tends to use sensors and operates all the time. The system uses feedback where the data is processed in time to turn on a device so that the environment is maintained.

Used in air traffic control, chemical plant, nuclear power plant.

2.8 – Factors affecting the use of ICT
&
2.9 – The consequences of the use of ICT

The two final sections of this unit can be blocked together; one looks at the factors affecting ICT but discussions regarding the use of ICT and the problems associated with it can easily be added. The section below has therefore been written to include some of the consequences of ICT.

The new examination does not set specific areas for the factors affecting the use of ICT, but below are some examples. The type of questions that will be set in the new examination will be far more open than the previous specification, so whereas in the past questions related to set topics, from summer 2008 the questions will relate to any topic. The use of ICT can be influenced by the following factors:

- Cultural
- Economic
- Environmental
- Ethical
- Legal
- Social

Impact of ICT on Education

Teachers have to adapt to teaching using computers as more students concentrate on the area of ICT at all levels from Key Stage 1 to degree level, or have computers at home. ICT has become an essential part of managing schools and colleges efficiently and more and more of the general tasks are being carried out using ICT. This can take the form of administration work like timetabling, registration or teaching via computer; this latter term is **"E-Learning".** New methods of teaching resources are constantly being created to allow the student to interact with their subject through video clips, online quizzes and real-time chat, e.g. Video Conferencing or Teleconferencing. In some areas students are able to contact their teachers 24 hours a day, 365 days a year using virtual learning environments; this has many positive points as the students can ask for help as they are working rather than waiting until the next time they see their teachers in person. It also has drawbacks as the teacher is effectively on call 24 hours a day. Using computers to take over the everyday tasks in school helps the school to become far more economic, allowing teachers to teach. However, using computers more and more causes health problems for the teachers and administration staff as well as students; this needs to be monitored closely by the school so that Health and Safety laws are not broken.

Advantages

- Work produced on an ICT system is more presentable than handwriting.
- It is more efficient and less time consuming than traditional paper methods.
- Students can work at their own pace.
- Constant monitoring can be set up to help the students to progress.
- Paperwork is reduced.
- Working practices become more efficient.
- Staff can find a student very quickly using online timetables.
- Electronic registration monitors where students are at any time of the day.
- Systems can easily control and monitor attendance.

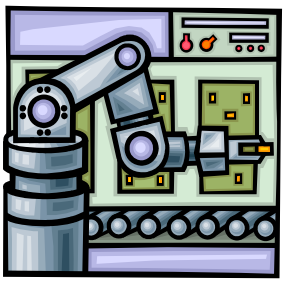
Disadvantages

- Students and staff may become more isolated.
- Students lose the contact of working with the teacher and this can lead to a lack of motivation.
- Teachers may be more knowledgeable than a computer.
- Computers automatically correct mistakes, e.g. spelling errors that students may otherwise not notice.
- There is a large increase in plagiarism, as using a computer is too easy and this makes people lazy.
- Health problems can result from using computers for long periods of time.
- Can lead to a 'Big Brother' situation.

Impact of ICT on Manufacturing

Modern manufacture makes use of:

- **Computer Aided Design / Computer Aided Manufacture (CAD/CAM)**
  This is the creation of 2D and 3D designs using a computer. These designs can then be saved and later manipulated without redrawing from scratch. 2D designs can easily be changed into 3D designs. Once the design is complete the computerised tools can then make it a reality.
- **Just in Time (JIT)**
  A computerised system that organises workflow, allowing for **rapid**, **high quality** and **flexible** production from raw material to product, thus minimising **waste** and **stock levels**.
- **Stock Management**
  A computerised system that controls the holding of stock, telling you about how many products are left, how many have been ordered, if the company needs any more of the product to fit the demand of production.
- **Order Management**
  It helps to control the manufacturing process, from ordering raw materials to production and delivery of the goods. This system is designed to bring together suppliers and delivery.
- **Robots**
  These are most commonly used in car production where the computer controls the mechanics of a robotic arm to perform a task. Robots, however, are now used in a number of different tasks which would be dangerous or impracticable for a person to perform.



Robotics is an area that makes for a good answer to a question as it relates to many of the above areas.

For example: robots are usually employed in a company as they reduce costs in the long run. Robots are expensive to set up but eventually they cost a great deal less than the work force that they have replaced. They can operate with a minimum number of operations staff, 24 hours a day, 365 days a year. The main problem with bringing in robots is that operations staff are replaced by the robots and then a large number of staff is made redundant, although some of these staff will become maintenance workers helping to keep the robots operating. A company that employs robots increases their fuel bills as more electricity is wasted. This increases the carbon footprint and therefore is harmful to the environment. Robots are far more precise than humans; in fact, once a robot is programmed it will continue to do the same task, with the same precision, time and time again. Some robots, nowadays, carry out minor laser operations on humans.

A disadvantage of using robots is the high cost to install and maintain. If a slight change is needed to the creation of the product then a human can easily make the change, however, a robot will need to be re-programmed, losing valuable production time and money. Robots may make good economic sense, however, humans lose the skills to produce the product and if a robot breaks down then it is becoming increasingly difficult to carry on the process without them.

Impact of ICT in Banking

Banking has changed over the past few years with more and more people undertaking telephone or internet banking than ever before. Again this is a good topic to cover in an examination, as it covers many of the factors listed above.

Online and telephone banking is available 24 hours a day. This allows the user to pay for goods or transfer money at the touch of a button, but they cannot withdraw money from a bank. Money has been changed to an electronic format which means that it cannot be easily stolen, although someone breaking into an account can transfer money out of that account without anyone being the wiser. If people want physical money they can visit a cash machine, which can be found in shops as well as outside banks, and then use a bank card to withdraw money. Electronic banking therefore reduces the carbon footprint as people do not need to travel to a bank in order to pay bills. When we shop we pay by credit card which instantly transfers money from our accounts to the shop's account.

Use of online banking has an economic effect, as it makes shopping easier and therefore fuels the economy, although it does increase debt as people do not realise how much they are spending. Online shopping allows people to sit at home and shop, increasing laziness and making them recluses; it does, however, allow for goods to be bought from all over the world. Banks are closed and staff made redundant as they are no longer needed due to online banking, although some jobs are being transferred to call centres. The main disadvantage of banking in this way is that it increases online fraud and customers tend to lose control of their money.

Online Banking Services allow customers to:
- Check account balances.
- Transfer funds.
- Pay bills.
- Apply for loans / mortgages.
- Trade stocks or shares.

Cash Machine (ATM)
Gives you an access to cash and your account globally 24/7. Each transaction is recorded to your account almost instantly (real time).

Debit Cards
When your bankcard is swiped, the balance is checked by the PDQ card machine and if there are sufficient funds in the account, the amount of the purchase is automatically debited from the account and transferred into the account of the shop.

Credit Cards
When your card is swiped, the money is removed from a credit bank, which you have to pay back. If you fail to do this then you are charged interest.

Direct Debit
Purchases that are the same amount of money paid on a regular basis can be paid by Direct Debit from your account to the receiver's account, e.g. an electricity bill.

Impact of ICT in Health

Equipment:
1. Scanners / X Ray – ICT processes the images into a readable format.
2. Microchips – can be installed internally, e.g. a pace maker.
3. Life Saving – e.g. life-support machine monitors the output of a human's functions.
4. Laser – skin grafts and operations can be performed to a precise degree.
5. Administration systems can help monitor patients.

Records:
Database – patient records are kept electronically and can be transferred from doctor to hospital. Regional trends and family connections can be analysed.

Internet:
Web doctor sites can be used to gather information, or for diagnostics of illnesses; these tend to be expert systems. Medical articles can be obtained and research followed. However, not all information is accurate.

The impact of ICT on offices

Working from home or teleworking is becoming more popular with the introduction of faster communication links and broadband. This allows an employee to remain in touch with the office whilst working from home. This reduces the carbon footprint and traffic levels, as people do not need to travel to work in order to do their business. A result of this is the reduction in the size of offices that need to be built, reducing the carbon footprint even further and helping the environment. Someone who teleworks can work flexibly around their own family in an environment that is familiar; however, sometimes this flexibility can clash with family demands and as a result teleworking can be less efficient than normal working.

Advantages:
- Flexi-time.
- Home comforts.
- No commuting.
- Reduces carbon footprint and helps the environment.

Disadvantages:
- Feeling of isolation.
- No human contact to discuss work issues.
- Self-control needed to work productively.
- Homely distractions such as children or pets.