SECTION 6
THE EFFECTS OF USING ICT

(a) Software Copyright- Meaning & Importance
(b) Threats to Computer System- How to protect from them
   - Computer Virus
   - Hacking
(c) Effects of ICT on Employment
(d) Effects of microprocessor-controlled devices in the home,
(e) Capabilities and Limitations of ICT
(f) Internet Developments
   Web 2.0,
   Blogs & Wikis,
   Digital Media uploading Websites
   Social Networking websites
(g) Issues relating to information found on the internet
   Security of data transfer
   Phishing, Pharming and SPAM
(h) Health problems related to the prolonged use of ICT equipment,
   Repetitive strain injury (RSI),
   back problems, eye problems
   some simple strategies for preventing these problems
(i) Safety issues related to using computers and measures for preventing accidents
SECTION 6: THE EFFECTS OF USING ICT

ICT can affect people positively or negatively. Some of the positive ICT effects include an increase in information access, better and cheaper communication services and world globalisation. The negative effects include the high cost of research and implementation of new technology, and sometimes it poses a security threat to personal data, creating opportunities for identity theft to occur.

Software Piracy: The unauthorized copying of software. A term used to describe the act of illegally using, copying or distributing software without purchasing the software or having the legal rights. The majority of software purchased today is purchased as a one-site license, meaning that only one computer may have that software installed on it at one time. Copying that software to multiple computers or sharing it with your friend without multiple licenses is considered illegal and is considered software piracy.

Software piracy is now being treated as a very serious crime, and the penalties can be severe

Software Copyright: Software copyright is used by proprietary software companies to prevent the unauthorized copying of their software. Protection for any published work or software that helps to prevent that work or software from being used without prior authorization. A copyright may be indicated by the word "Copyright", or a C surrounded by a circle (©), followed by the date of when the work was published, and finally the author of the work. When work is copyrighted, it may not be reproduced in any fashion unless the owner of the work grants proper rights.

Laws exist to help prevent the developers of software from having their work downloaded or copied by others for free.


• This makes it a criminal offence to copy or steal software. This includes:
  – Copying or distributing software or manuals without the permission of the copyright owner (usually the software developer).
  – Using purchased software covered by copyright on more than one computer unless this is permitted by the software licence.
  – Encouraging or allowing people to copy or distribute illegal copies of software.
  – A person guilty of an offence under this act may be sent to prison for up to ten years and be fined!
**Prevention of software piracy**

Software companies take many steps to stop software piracy:

- **A registration key** - a unique series of letters and numbers that is asked for when running the program. The software will not run if the registration key is not typed in correctly and online multiplayer games will not to run if another user is online who has used the same key.
- **A phone or Internet activation code** - this requires the user to call a number or go online to register the product. They then receive a unique computer-specific serial number.
- **Encryption** - data can be scrambled up and cannot be read without the correct software.
- **A Dongle** - a piece of hardware that must be plugged into the computer to run the software. Each one contains a unique electronic serial number and as they are expensive to produce they are mostly used to protect high-end software packages.
- **Details of the user are built into the software** - when the software is run it displays the original users name. This does not prevent the copying but it makes is obvious that the copy is illegal.
- **A Keyfile** - a small file with a unique code that is placed in the same directory as the program. If the code is not valid then the software will not run.
- **Copy protection** - the disk *(or CD-Rom)* may be formatted in a special way so it cannot easily be copied.
- **Restricting the number of installations** - each installation is recorded on an installation disk and only a certain number are allowed.

**Computer Virus**: Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation. Viruses can also replicate themselves. Computer viruses are often spread by attachments in email messages or instant messaging messages. That is why it is essential that you never open email attachments unless you know who it's from and you are expecting it.

**Types of Virus**

**Trojan Horse**

A program written to deliver a malicious program that may then cause destruction to your computer. A Trojan horse is delivered by someone or hidden within another program that may seem harmless.

**Spyware**

A program written to monitor your actions on a computer. A common type of spyware is a key-logger program. This program can record every key stroke and mouse click you make. Spyware can be delivered via a Trojan horse program. Some spyware is not meant to be malicious, such as tracking cookies. A tracking cookie tracks your internet usage and sends the information back to its source.
Adware

Adware is a form of malware. One word - pop-ups. Adware is designed to pop up advertisements. Adware can be very annoying.

Worm

A worm is a program very similar to a virus; it has the ability to self-replicate and can lead to negative effects on your system. These generally spread through e-mails and networks. They do not infect files or damage them, but they replicate so fast that the entire network may collapse. But they can be detected and eliminated by an antivirus software.

Boot Sector Virus

Not so common anymore, but they were nasty little programs that got loaded into your master boot record. Most commonly spread by floppy disks. These viruses could then launch themselves before your operating system even loaded. Today most BIOS prevents code from being written to the boot sector.

Time Bomb

They are not considered viruses because they do not replicate. They are not even programs in their own right, but rather camouflaged segments of other programs. They are only executed when a certain predefined condition is met. Their objective is to destroy data on the computer once certain conditions have been met. Logic bombs go undetected until launched, the results can be destructive, and your entire data can be deleted!

How do you know if computer has been infected?

If you open and run an infected program or attachment on your computer, you might not realize that you've introduced a virus until you notice something isn't quite right. Here are a few indicators that your computer might be infected:

- Your computer runs more slowly than normal
- Your computer stops responding or freezes often
- Your computer crashes and restarts every few minutes
- Your computer restarts on its own and then fails to run normally
- Applications on your computer don't work correctly
- Disks or disk drives are inaccessible
- You can't print correctly
- You see unusual error messages
- You see distorted menus and dialog boxes
Protection against viruses
When it comes to protecting your computer from virus the proverb „Precaution is better than cure” is very much applicable. Some precautions could be
- Any executable .EXE files should not be opened unless you trust the sources.
- Never open unsolicited e-mail.
- Use reliable virus protection software.
- Always use computer firewall.
- Avoid using flash discs, floppy disc which were used on other computer. In case you cannot avoid, do a virus scan before using these devices.
- Viruses may spread through infected floppy discs, flash drives (pen drives), downloads from internet or through e-mails.

Hacking
Hacking means attempting to gain unauthorized access to a computer system. These people are known as 'hackers'

Why do hackers hack?
- curiosity
- challenge - can they get through the system's defences?
- to access data, usually because the data has value
- to steal financial information such as your credit card number, or the password to your bank account, in order to use that information to make purchases.

Protect yourself against hackers
- Use strong passwords to protect your user login account
- Never reveal your login password to anyone else
- Place a firewall between your computer and any network
- Disconnect from networks (e.g. the internet) when you are not using them
- Encrypt any sensitive information (just in case they get in)

Encryption makes the files on you system unreadable if the user does not know the password to un-encrypt them. If someone try's to read an encrypted file they will just see random junk instead of the real data.

Credit Card/ATM Card use Encryption technique to prevent data theft. Even if your ATM Card hacked by Hacker he will not be able to use it as data is encrypted

Firewall: A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets.
All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

**Impact of ICT on Employment**

ICT has widely changed the employment pattern over the years. It not only changed the employment but also the working environment. There are both positive and negative impact of it.

**Positive**

**New Jobs has been created**

- Engineers are needed to build the new computerised machines.
- Programmers are needed to write the new programs that the computers run.
- Systems analysts are needed to design the new computerised systems.
- Skilled workers are needed to operate the new computerised machinery.
- Skilled workers are needed to use new software such as graphics packages, web-design software and CAD programs.
- More staff may be needed because of the increased business generated by improved efficiency.

**Change in Working Style**

- People may **work less hours** as a result of the increased efficiency of automation and the introduction of ICT into their workplace. This has therefore led to an increase in leisure time.
- Many people can now **work from home** using teleworking.
- Students can **educate themselves** more easily due to the huge amount of educational software resources and information now available, much of it interactive and allowing them to self-assess.
- It has made it possible for **easier work interactions** through email and video conferencing, created workstations, improved communication in the workplace and made remote working possible, among others.
- **Safer environment** as most the difficult jobs are done with the help of computerized machine for example use of Robotics in Car Manufacturing unit.
Negative
The introduction of information technology has caused some unemployment, for example:
- Computer-controlled warehouses need only a handful of staff to operate them.
- Computer-controlled robots are now common on production lines, replacing human workers.
- The old skills of workers in the printing industry are now out of date.
- Some jobs have disappeared as they can now be done automatically, eg marking multiple choice exam papers.

Teleworking
Teleworking, sometimes called telecommuting, means working from home using modern technology to keep in touch with your business. Jobs can be relocated to places where it is more attractive, more convenient or cheaper to live.

Technology required for teleworking
- a computer with internet access
- an email account

Some teleworkers may also use:
- a fax machine
- a mobile phone
- videoconferencing equipment

Advantages for the employer
- Office running costs and overheads (rates, electricity, heating etc) can be reduced, which in turn may reduce the need for office space.
- Travel-related problems may be reduced, ie staff being unable to get into work due to rail/road delays.
- It may tempt better staff to come and work for the company.

Disadvantage for the employer
- Employers need to be able to trust their staff and be prepared to have less direct control over them.

Advantages for the employee
- work in a comfortable environment - their home
- no commute and no travel costs
- work around their family’s needs

Disadvantages for the employee
- less human interaction - fewer opportunities to meet people, share ideas with etc.
- more difficult to work as part of a team, especially if they’re all office based
- greater temptation to spend time on non-work-related activities
- difficult to separate personal life from work
Video conferencing

Video conferencing means using computers to provide a video-link between two or more people. Instead of just talking to someone by telephone, you are able to see them as well.

Equipment

The following is needed to take part in a video conference call:

- a computer
- a web cam
- a microphone (most webcams have a microphone built-in)
- speakers
- High Speed Broadband access
- video conferencing software

It is possible to buy a special video conferencing machine just for this purpose.

Advantages of video conferencing

- Meetings can take place without leaving the office.
- Travel costs and the time taken to travel can be reduced significantly.
- Meetings can be called instantly worldwide with little notice.
- Delegates can still attend meetings even if they are physically unable to.

Disadvantages of video conferencing

- May not be as productive as a discussion around a table.
- Confidential documents may need to be viewed and signed in person.
- There will always be times when you need to be able to meet face to face.

Why companies invest in new technology: As a factory invests in computerised equipment some of its workers may be made redundant. Its productivity rises as its labour costs are reduced and it will become more competitive.

What can happen if companies do not make this investment: If a company does not invest in computerised equipment then higher labour costs and lower productivity will means its products will be less competitive. This could result in the company failing and jobs being lost anyway. This is an issue that employers, trade unions and governments have to face.

Effects of microprocessor-controlled devices in the home,

Microprocessor is a small Central Processing Unit built into a single chip. Usually powerful microprocessors are used in PCs but less powerful ones are used in many typical everyday devices in home => microcontrollers

In a single ‘chip’, a microcontroller contains:
A CPU
Some RAM
Some ROM (Used for storing the devices software)
Some of them are labour-saving devices (Requiring less human input):
Programmable microwave ovens
Programmable washing machines
Home security systems
Mobile telephones

Effect of microprocessor controlled Devices at home

- The effects on **leisure time** - microprocessor controlled domestic appliances such as washing machines, cookers, heating systems etc. do not need direct human control because they have timers, operating programs and safety checks built in. This means the user can leave them to complete their tasks so they have more leisure time.
- The effects on **social interaction** - from the comfort of the home people can communicate in many more ways than the traditional telephone and postal service.
  - **Email** allows fast efficient communication with the ability to send files as attachments and email many people at the same time.
  - **Online messaging** allows users to sent text, images and files in real time, as well as communicate via voice and video.
  - **Wireless phones** and **mobile phones** allow interaction by telephone conversations from any room or the garden.
  - **SMS** (Short Messaging Service) text messages, images and video clips to be sent between mobile phones and computers.
  - **Answer machines** allow messages to be left for users who cannot answer the telephone.
  - **Social interaction websites** allow users to interact by leaving messages and adding comments to blogs. Users can also upload and share image and video files.
- The effects on **the need to leave the home** - computers linked to the Internet have greatly reduced the need for people to leave the home.
  - **Entertainment** - music and games can be downloaded. Movies can be downloaded and this, along with Interactive digital television, means there is no need to go to the cinema or video rental shop.
  - **Goods** - these can be easily ordered from online stores and delivered to the home.
  - **Food** - takeaway food and groceries can be ordered online and delivered directly to the door.
  - **Services** - banking, ordering insurance and many other services can be carried out over the telephone or the Internet.

### Capabilities and Limitations of ICT

#### Capabilities

**Makes communications easy**
ICT has helped in the revolution of communication, and also in electronic communication. Like emails, text messages have enabled the society to become more connected in addition to enabling communication and mass communication easier & faster
Processing Speed has increased many folds
With a speed reaching up to fifty million operations per second, a computer can process data faster than any other machine designed to perform a similar task.

Repetitiveness: A computer can perform the same operation a million times in exactly the same way. The various operations are executed automatically by way of stored computer programs.

Accuracy of Data
High-speed processing by a computer is accompanied by high-accuracy results. A computer can be considered 100% accurate. The electronic circuitry of computers is such that, when the machines are fed with correct instructions or data and when the incoming data is error-free, the accuracy of the output is relatively assured.

Quick Information with the use of internet information flow become very easier, Satellite imaging, medical research and scientific research searches and sorts out the data with computers one can get the information quickly E.g. Google

Provides large storage of data
Computers can store much more data digitally in their hard drives than we can in our heads and paper files. E.g. The internet, USB sticks, DVDs, Hard drives, etc

Limitations of ICT
1. A computer cannot generate information on its own. While it is true that a computer has the capacity to put together information from many sources, it can only do this if it has been programmed by man to do so.
2. A computer cannot correct wrong instruction. If a computer is fed with incorrect instructions or data, whether intentionally or unintentionally, it does not have the capability to detect mistakes and correct them. In computer language, this is known as GIGO (garbage in garbage out). This means that a computer that has been fed with a wrong set of instructions or data will similarly produce wrong information and wrong decisions. Therefore, any corrections must be done by the programmer.
3. A computer can only do what you tell it to do.
4. Information overload (e.g. people can be flooded with Email)
5. Computer crime (hacking, viruses)
6. Lack of hardware and software standards
Internet Developments

Web 2.0 is the term given to describe a second generation of the World Wide Web that is focused on the ability for people to collaborate and share information online. Web 2.0 basically refers to the transition from static HTML Web pages to a more dynamic Web that is more organized and is based on serving Web applications to users. Other improved functionality of Web 2.0 includes open communication with an emphasis on Web-based communities of users, and more open sharing of information.

- share information (e.g. notes and photos on Facebook)
- interact (add comments, chat, etc.)
- collaborate on content (e.g. creating pages on Wikipedia)
- create their own content (e.g. videos on YouTube)

Wiki is usually a web application which allows people to add, modify, or delete content in a collaboration with others. Text is usually written using a simplified markup language or a rich-text editor. While a wiki is a type of content management system, where content is created without any defined owner or leader, and wikis have little implicit structure, allowing structure to emerge according to the needs of the users. Example Wikipedia

Blog originally came from the word “we blog” or a “we log”. You can think of it as an online journal or diary, although blogs are used for much more now, like online journalism. Blog posts typically appear with the most recent blog post (or entry, post) first, just like a diary or journal. Blogs typically have an area for people to comment or respond to the blog post.

Social Networking service is a platform to build social networks or social relations among people who, for example, share interests, activities, backgrounds, or real-life connections. A social network service consists of a representation of each user (often a profile), his/her social links, and a variety of additional services. Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Example: Facebook, Twitter, Linkedin etc

<table>
<thead>
<tr>
<th>Blog</th>
<th>Wiki</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blogs are personal</td>
<td>Wiki are Open to collaboration</td>
</tr>
<tr>
<td>Content is considered to be static: once posted, the posting doesn't change</td>
<td>Content is not permanent, it can be revised by any one</td>
</tr>
<tr>
<td>A posting is owned by a poster</td>
<td>Topics are considered public space owned by all</td>
</tr>
<tr>
<td>blog achieves one to many communication</td>
<td>wiki achieves a many to many means of communication.</td>
</tr>
</tbody>
</table>
Digital Media Uploading Website  It is a website where the visitors can transfer media like videos, photos, podcasts and etc. on to a site from your computer to share with others. Usually other users can rate or comment on the media that is uploaded leading to these sites often being referred to as 'Social Media' sites.

All media upload sites have rules about the type of media that you can upload - you have to either own the copyright to the image / music / video yourself, or have permission from the copyright owner. Examples YouTube Flickr

Information on Internet

Information is probably the biggest advantage that Internet offers. Internet is a virtual treasure trove of information. Any kind of information on any topic under the sun is available on the Internet. The search engines like Google, Yahoo are at your service on the Internet. There is a huge amount of information available on the Internet for just about every subject known to man, ranging from government law and services, market information, new ideas and technical support.

Reliability of Information

The Internet and Web are not regulated - there is no organisation that controls who can create web pages or what those pages can contain. Anyone can create web pages and say anything they want to.

Which information to trust?

- Check several sources of information (go to lots of different websites). If they all say them same thing, it is likely to be true
- Stick to websites that belong to trusted organisations. If the website address ends in.gov.uk /gov.kw/gov.in it is more likely to be reliable than one like www.tomiscool.net
- Look at the spelling and grammar used. Reliable websites are usually checked for errors. Too many spelling errors mean it's probably not to be trusted.

Undesirable Information

Internet contains a lot of misleading information that may seem very convincing Because many people use internet as an information source, corporations are misusing internet to promote their interests.

There are also a huge number of websites that contain highly offensive, or illegal material. Avoiding this type of material can be tricky. Many organizations such as schools, some governments and also many parents, make use of web page filtering software. This software attempts to prevent offensive and illegal material being accessed.
Security of Data Transferred Using the Internet

Many websites, especially online shopping or online banking sites, require you to enter personal information, such as credit card numbers, social security IDs, etc. To make sure your data is safe, these websites use encryption - they are called secure websites.

You should always make sure that a website is secure before giving personal information...

The website URL (address) should begin with https://... (normal, unsecure sites have addresses that start with http://...)

Your web browser should show a closed padlock icon

Phishing

Phishing (password harvesting) is an illegal activity where someone attempts to acquire sensitive information such as user names, passwords and credit card information. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user’s information.

The purpose of the fraudulent sender is to "phish" for or entice people to share, their personal, financial, or password data. It’s then used to commit crimes.
What does a phishing email message look like?

Here is an example of what a phishing scam in an email message might look like.

Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Our system detected unusual Copyrights activity linked to your Facebook account, please follow the link bellow to fill the Copyright Law form:

http://www.facebook.com/application_form

Note: If you don’t fill the application your account will be permanently blocked.

Regards,

Facebook Copyrights Department

Pharming

“Pharming” is the term for when criminal hackers redirect Internet traffic from one Web site to a different, identical-looking site in order to trick you into entering your user name and password into the database on their fake site.

Why do they do it?

Criminals try to acquire your personal information in order to access your bank account, steal your identity, or commit other kinds of fraud in your name, so banking and similar financial sites are often the targets of these attacks.
How does pharming work?

- A hacker attacks a DNS server
- The hacker redirects traffic from the real website to his own fraudulent site
- The user types in the web address of the real site
- They are instead taken to the fake site – usually a bank or other ecommerce site.

Email spam, also known as junk email or unsolicited bulk email (UBE), is a subset of electronic spam involving nearly identical messages sent to numerous recipients by email. Clicking on links in spam email may send users to phishing web sites or sites that are hosting malware.
Health problems related to the prolonged use of ICT equipment

Stress

Working with a computer can be stressful in that the computer can handle data as quickly as the operator can enter it. In addition, the introduction of computer technology tends to de-personalize the work environment, reducing the opportunity of human contact, so that stress-relieving chat or gossip is no longer possible. Stressed employees are more susceptible to other health problems e.g. heart disease and ulcers. Stress, in itself, is an illness that can cause long-term absence from work. Stress in workplace is made worse by:

- Using computers to monitor employee’s performance
- Technophobia (the fear of computers by older staff and their concern that they will become de-skilled by the introduction of IT)
- Pagers, mobile phones, and laptops mean that an employee can never truly be away from the office.
- “Information overload” (computers can bombard people with more information than they can assimilate)

Repetitive Strain Injuries (RSI)

Repetitive Strain Injuries occur from repeated physical movements doing damage to tendons, nerves, muscles, and other soft body tissues. Occupations ranging from meatpackers to musicians have characteristic RSIs that can result from the typical tasks they perform.

What are the Symptoms?

- Tightness, discomfort, stiffness, soreness or burning in the hands, wrists, fingers, forearms, or elbows
- Tingling, coldness, or numbness in the hands
- Clumsiness or loss of strength and coordination in the hands
- Pain that wakes you up at night
- Feeling a need to massage your hands, wrists, and arms
- Pain in the upper back, shoulders, or neck associated with using the computer.

Preventions

- Keyboard should be separate from the VDU.
- Ergonomics Keyboard should be used
- Keyboard should have concave keys to prevent fingers slipping and reduce impact shock on fingertips, fingers, wrists, and arms.
- Wrist supports can also be used
- Workers should be allowed regular breaks.
Eye Strain

Concern about the effect on eyesight. VDU's have been blamed for causing eyestrain and there are claims that prolonged exposure can lead to the development of cataracts.

Preventions
- Use an anti-glare screen.
- Good lighting.
- Look away from the screen and at a distant object frequently.
- Have regular eye checks.

Radiation Hazards.

Computer equipment - particularly VDU's give of electromagnetic radiation. There is particular concern that this may lead to miscarriage or birth defects when pregnant women work for long periods at a VDU screen.

Preventions
- Low emission' monitors
- Use an anti-glare screen

Safety Issues

The rules for all electrical appliances apply in a computer room.

- There should be no trailing wires.
- Food and drink should not be placed near a machine.
- Electrical sockets must not be overloaded. Adequate space around the machine.
- Suitable heating and ventilation.
- Suitable lighting with no glare or reflections.
- Benches must be strong enough to support the computers.
- All electrical equipment must be tested for safety at regular intervals.