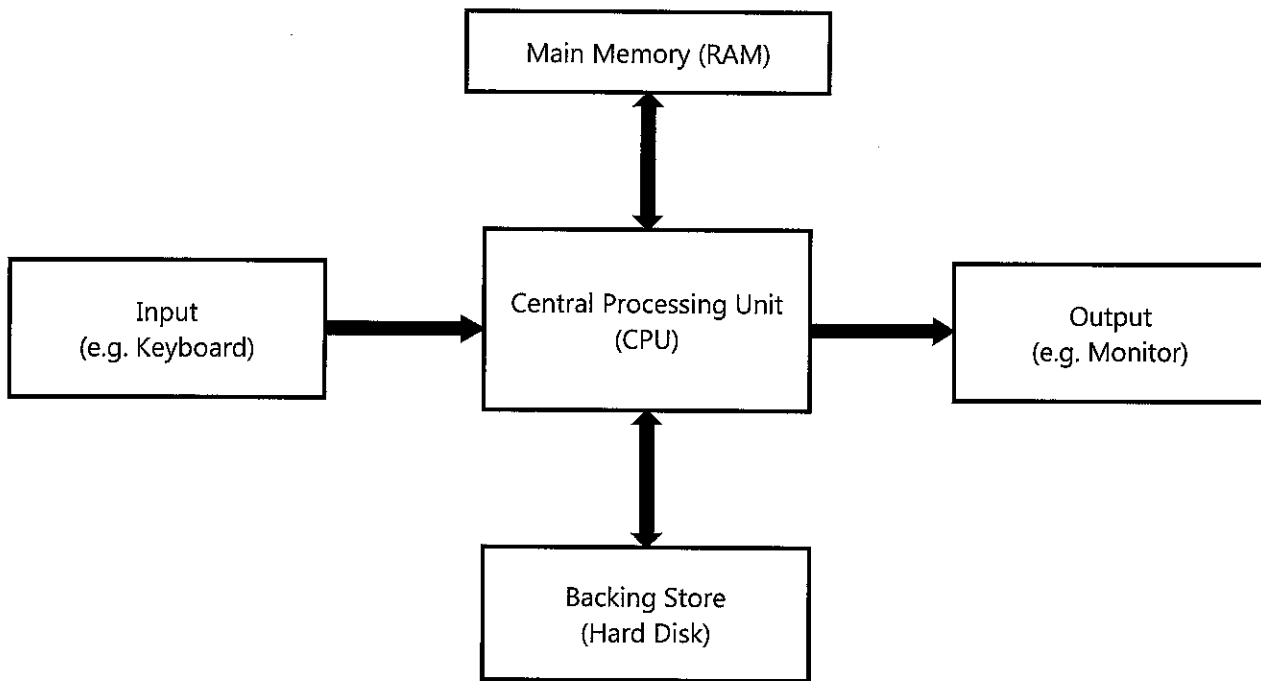


# 1 Fundamentals of Computer Systems

## 1.1 Computer Systems

The block diagram of a computer is shown below. All ICT systems have these same essential components. Some typical examples of devices have been included.

The main part of the system is the CPU, which is a single chip responsible for all the processing.



Computer hardware is the physical part of a computer, which includes digital circuitry, as distinguished from the applications software that is executed using the hardware. The processing hardware is necessary to gain a useable output from the system.

The input, auxiliary storage (sometimes known as a backing store) and output devices are known as peripherals, as they are NOT actually mounted on the system motherboard.

The backing store is normally a hard disk, which retains the data written on to it after the computer system has been switched off; it could include other storage devices such as flash memory and removable disks.

Computer systems need a power supply to convert mains alternating current (AC) into low-voltage direct current (DC) to supply power to the various internal components within the computer system.

The output from the ICT system is normally printed out by the user or displayed on a computer screen. However, other options include audible text or music output to a speaker.

**A computer system** operates with hardware and software to create a functional solution.

**Software** is the actual programs or coded instructions that make the computer run.

**Hardware** is the physical parts that make up a computer system.

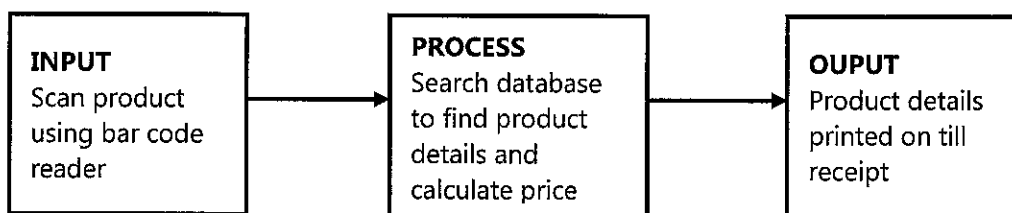
## Computer Systems

Any activity that involves input, processing and output is said to be a system; computer systems are based on input, processing and output:

**INPUT** – this is where data is entered into the computer system. It can be entered manually by using a keyboard to type in a part number into an online shopping form, for example, or by using a bar code reader to enter details of a sale at a supermarket.

**PROCESS** – this is where the data inputted is used to convert the input into a readable form; the bar code read in can be processed to obtain a description of the product, the size of the product and the price, for example.

**OUTPUT** – the information obtained by processing the data is presented to the user in a logical form; in the case of a supermarket, this could be to produce a display as the product is scanned in and all the products purchased could be printed out on a till receipt with suitable calculations when the shopping transaction is completed. A practical example of a computer system in a supermarket is shown in the block diagram below.



## 1.2 Importance of Computer Systems in the Modern World

Computer systems are an integral part of most people's lives; the following table gives examples of computer systems in both business and leisure.

**Embedded systems** are where a computer processor is integrated into a device for automatic control purposes.

Where Used	Detail	Examples
<b>Embedded systems</b>	Computers in the home are used to automatically control various systems and reduce workload.	Examples are: washing machines, central heating control, burglar alarm, dishwasher and security cameras and lighting.
<b>Home entertainment and communications</b>	Most modern households use a range of computer-driven devices for entertainment and communication. Smartphones are widely used to surf the Internet, send email and make calls.	Examples are: laptop, tablet computer, netbook, iPhone, DVD player, hard disk TV recorder, TV and computer games, online shopping, etc.
<b>Commerce and business</b>	Most organisations use computer systems widely; both for basic office functioning, interpersonal communication and ecommerce.	Main examples are: teleworking, videoconferencing, cloud computing, collaborative working, website creation and online sales.
<b>Medical systems</b>	Doctors and hospitals use computer systems to treat patients and diagnose illnesses.	Examples are: administration, diagnostics with scanners and radio therapy.

Computer systems are also used in education and schools, banking and finance, government, leisure clubs and venues, and military application.

## 1.3 Computer System Reliability

It is necessary for computer systems to be reliable and robust as society has become that much more dependent upon them.

Reliability of computer systems can be improved by purchasing high-quality components and fully testing the system during development.

Robustness can be improved by using verification and validation techniques to help prevent abnormal inputs. Also, when the computer system is commissioned, robustness can be improved by testing for erroneous inputs and then preventing them in future using either hardware or software techniques.

**Reliability** is the ability of the computer system to perform the required functions without failure.

**Robustness** is the ability of a computer system to continue to operate normally despite abnormal inputs or calculations.

It is very important that computer systems are both reliable and robust as:

- Systems that aren't reliable might fail or crash. The consequences could be serious in a medical situation or trade could be lost in an ecommerce context.
- Systems that aren't robust might 'hang', which would prevent a customer completing a transaction.

## 1.4 Professional Standards

In ICT, standards are crucial in the areas of compatibility and interoperability between computer systems, which are defined as:

- When two machines from either a different manufacturer or specification run the same programs, they are considered to be software **compatible**.
- **Interoperability** enables different systems to work together and exchange data, and this is achieved by using common standards. This feature is mainly made use of in networking where two incompatible computers can interoperate if they both support the same networking protocol, such as the Internet's TCP/IP.

**Compatibility** is the ability of two different specification computers to run the same software.

**Interoperability** is the ability of different systems to exchange data using common standards.

The following standards are used within the computer industry:

- **Industry standards** are where the hardware or software is endorsed by a standards organisation, such as America's IEEE (Institution of Electrical and Electronics Engineers) and the ISO (International Standards Organisation). A typical benefit of industry standards is that universal serial bus (USB) connecting cables can be obtained from a variety of manufacturers since they have a standard configuration, allowing the organisation to choose a cable at the right quality and price.
- **De facto standards** exist where they have been adopted by a large sector of the ICT industry due to dominance in the market; for example, the QWERTY keyboard layout has become the standard over a period of time.
- **Open standards** are sometimes linked to the term 'open source'; this is where the user has the option to modify the source for their own purpose if they have the time and the necessary expertise. Typical examples of open standards are the operating system Linux and programming software Python.
- **Proprietary standards**, sometimes known as closed source, are owned and defined by a market leader; a typical example is Apple Computers that control the hardware and operating system for their computer devices, such as the iPad, iPhone, MacBook and iPod.



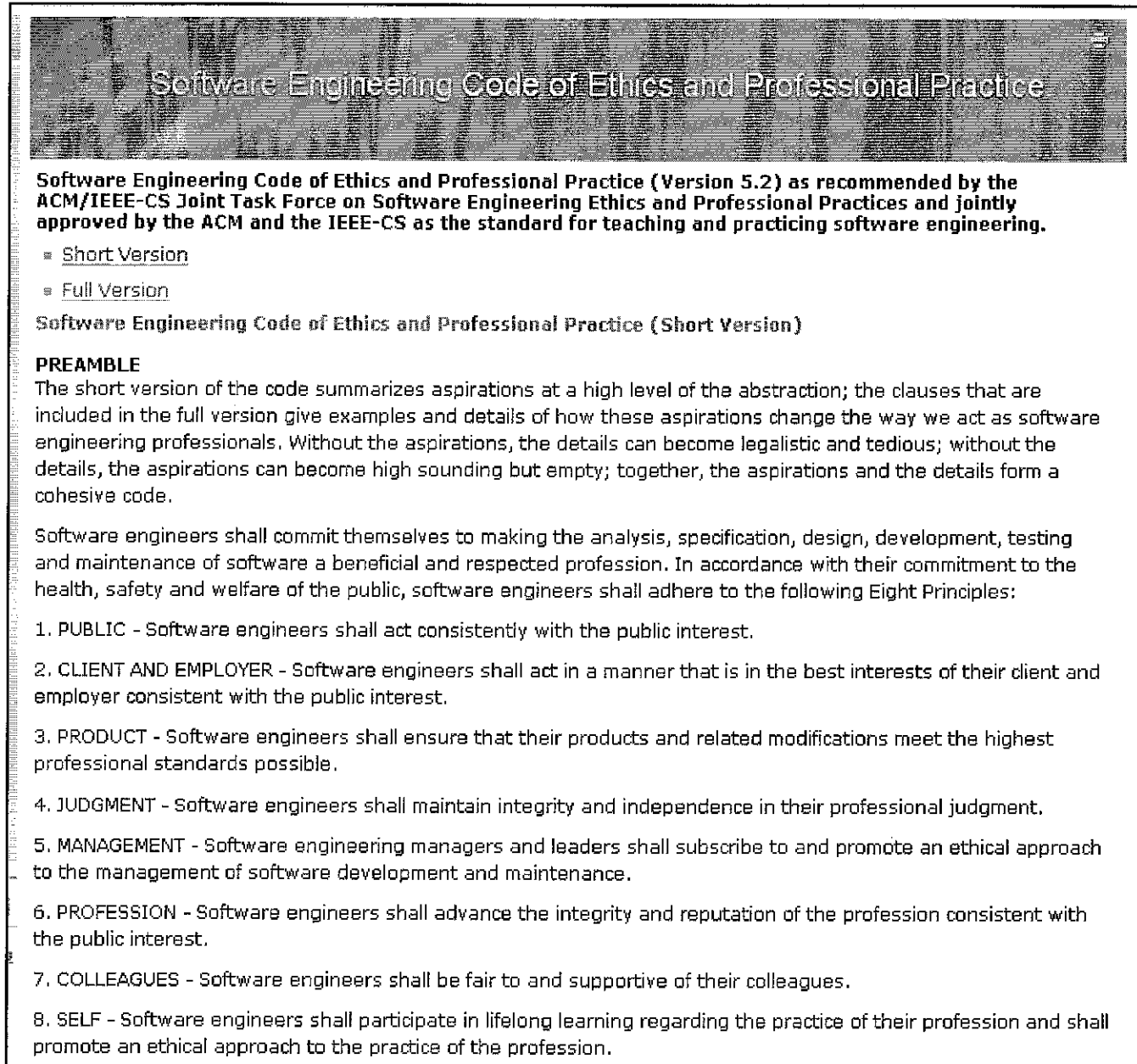
## 1.5 Ethical, Environmental and Legal Considerations

### Ethical Considerations

There are many definitions of ethical standards, for example 'it is a set of principles to promote what is good for individuals and society'.

Ethical standards might be different for an individual based on what they consider to be 'right' or 'wrong'.

**Ethics** is a set of principles to promote what is good for individuals and society.



The screenshot displays the title page of the 'Software Engineering Code of Ethics and Professional Practice (Version 5.2)'. The title is centered at the top in a large, bold, serif font. Below the title, there is a subtitle in a smaller, bold, sans-serif font: 'Software Engineering Code of Ethics and Professional Practice (Version 5.2) as recommended by the ACM/IEEE-CS Joint Task Force on Software Engineering Ethics and Professional Practices and jointly approved by the ACM and the IEEE-CS as the standard for teaching and practicing software engineering.' Underneath the subtitle, there are two bullet points: '• [Short Version](#)' and '• [Full Version](#)'. The main heading of the document is 'Software Engineering Code of Ethics and Professional Practice (Short Version)'. Below this, the word 'PREAMBLE' is written in all caps. The preamble text follows, explaining the purpose of the code. At the end of the preamble, it states 'Software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession. In accordance with their commitment to the health, safety and welfare of the public, software engineers shall adhere to the following Eight Principles:'. This is followed by a numbered list of eight principles, each with a brief description of the expected behavior.

**Software Engineering Code of Ethics and Professional Practice (Version 5.2) as recommended by the ACM/IEEE-CS Joint Task Force on Software Engineering Ethics and Professional Practices and jointly approved by the ACM and the IEEE-CS as the standard for teaching and practicing software engineering.**

- [Short Version](#)
- [Full Version](#)

**Software Engineering Code of Ethics and Professional Practice (Short Version)**

**PREAMBLE**

The short version of the code summarizes aspirations at a high level of the abstraction; the clauses that are included in the full version give examples and details of how these aspirations change the way we act as software engineering professionals. Without the aspirations, the details can become legalistic and tedious; without the details, the aspirations can become high sounding but empty; together, the aspirations and the details form a cohesive code.

Software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession. In accordance with their commitment to the health, safety and welfare of the public, software engineers shall adhere to the following Eight Principles:

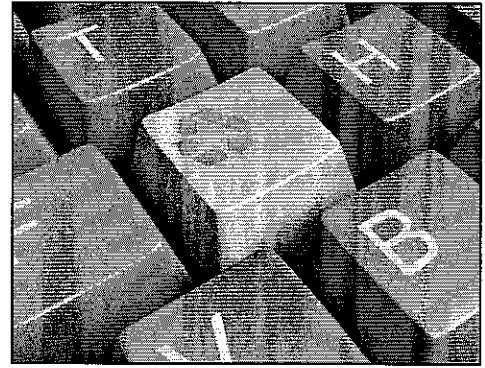
1. PUBLIC - Software engineers shall act consistently with the public interest.
2. CLIENT AND EMPLOYER - Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.
3. PRODUCT - Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
4. JUDGMENT - Software engineers shall maintain integrity and independence in their professional judgment.
5. MANAGEMENT - Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
6. PROFESSION - Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
7. COLLEAGUES - Software engineers shall be fair to and supportive of their colleagues.
8. SELF - Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

The screenshot above shows a widely used Software Engineering Code of Ethics and Professional Practice created by ACM (Association for Computer Machinery) and the IEEE (Institute of Electrical and Electronic Engineering).

Further details can be found at [www.acm.org/about/se-code#short](http://www.acm.org/about/se-code#short)

## Environmental Considerations

The computer systems developer needs to take account of the following environmental considerations:



### Recycling/Disposal of Digital Devices

- Recycling can have many benefits in protecting the environment as it reduces the amount of landfill sites that are needed, which is useful since we are running out of landfill space.
- It is important that computer users dispose of their old digital devices safely by using the local authority waste disposal sites. In most cases, the user should delete any data from either their computer hard disks or from the SIM card on their mobile phone.
- Old digital devices can also be recycled to less developed countries to extend their useful working life.

### Climate Change and Energy Usage

Computers use a large amount of energy; much of this energy is used in cooling electronic devices and systems. This is especially true in data centres where air conditioning is used to maintain a correct working environment.

Energy supplies are expensive and so it is important to make energy use efficient; this can be achieved by reducing the heat created in new computer systems. In some cases, it is possible to reuse the waste heat from data centres to heat other parts of the building and so reduce the organisation's overall energy usage and the impact on climate change.



Computer technology also makes an impact on reducing the damage to the environment by making use of automatic energy-reduction techniques within the workplace:

- Lights can be switched off automatically in individual offices when no one is in the room.
- Improved heating controls automatically take account of which rooms need to be heated and at what level.
- The use of low-energy devices for lighting is also making a contribution to energy reduction.

### Energy Usage Research Task

Check out the Computer Weekly article on green computing:

[www.computerweekly.com/guides/Using-green-computing-for-improving-energy-efficiency](http://www.computerweekly.com/guides/Using-green-computing-for-improving-energy-efficiency)

Check out this article on reducing computer energy usage:

[www.mnn.com/green-tech/computers/stories/5-tips-for-reducing-your-computers-energy-use](http://www.mnn.com/green-tech/computers/stories/5-tips-for-reducing-your-computers-energy-use)



## Sustainability

The sustainability of finite resources can be maintained in the computer industry by increasing the use of sustainable resources in the following ways:

- Operating the business based on a paper-free approach; for example, using online documentation rather than printing out user guides.
- Making use of electronic communication (SMS, social networking, mobile phone, emails, etc.) to increase the speed of communication rather than making use of the postage service.
- Making use of videoconferencing and teleworking to reduce the amount of commuting needed in business and to reduce fuel costs and consumption.

**Sustainability** is a method of resource usage that aims to meet current needs and those of future generations.

## Legal Considerations

The following legislation is important when creating computer systems:

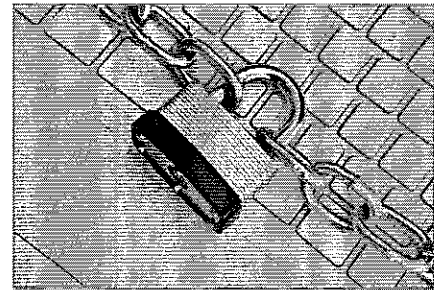
- Data Protection Act
- Copyright Law
- Computer Misuse Act

### Data Protection Act 1998

The Data Protection Act was introduced to ensure that the data held on clients conformed to certain principles such as: being held securely, being up to date and not being kept longer than necessary.

Keeping data secure is a key feature of this legislation and so, when developing computer software applications, it is necessary to add a range of software methods to help protect client data such as:

- **Passwords** entered into software applications should only be accepted if they are strong and so are more difficult to break; strong passwords are created by using mixtures of numbers, letters and symbols, using lower case and upper case, so that the final password does not look like a word.
- **Encryption** is used to make stored data more secure, by making it unreadable to people who do not have the key to decode it. This method is commonly used to protect data transmitted over the Internet.
- **Selective drop-down menus** are sometimes used as a security method to add letters for a password, rather than just typing them; this prevents key-logging software from viewing the systems and gaining access to important passwords.



### Copyright Design and Patents Act 1988

The Copyright Design and Patents Act introduced in 1988 aimed to protect the intellectual property of individuals and organisations that create and produce materials based on their own individual ideas.

The computing industry has grown tremendously in recent years with a great many new concepts and innovations. Copyright legislation is useful in protecting the following aspects of computer technology:

- **Software piracy** is the illegal copying of software for either personal use or business use.
- **Theft of hardware and software ideas and innovations.** In an industry that moves so fast there is seldom time to patent your invention before you release it on the open market. Many organisations purchase their rivals' products with the express purpose of copying their ideas, which saves them considerable expense on research and development.



Protecting your copyright is especially worthwhile when you or your organisation have invented a new hardware or software concept.

There are many websites that can help the creator to protect and patent their work. The main implication for ICT organisations is that they make the public aware of their intellectual property rights; this can be achieved by ensuring that they include documentation with their products, stating that their designs are copyrighted, can't be modified, copied or to use 'reverse engineering' techniques to produce replicas.

### Computer Misuse Act 1990

The Computer Misuse Act was introduced with the express purpose of preventing attacks on ICT systems to commit crimes or to damage the system; this legislation made hacking and the introduction of a computer virus into criminal offences.

**Hacking** is the practice of breaking into secure computer systems.

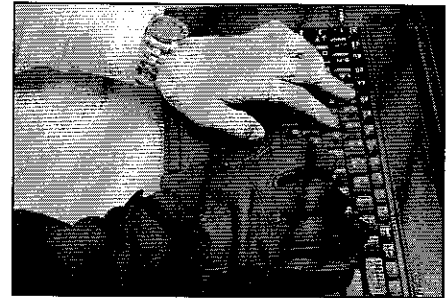
**Viruses** are programs designed to cause damage to a computer

A **firewall** is used to prevent unauthorised requests from hackers to gain access to the network or computer systems via the Internet.

**Spyware** are programs that run in a computer system to gather information and pass it on to other interested parties.

**Hacking** is the practice of breaking into computer systems and it is essential that preventative measures are taken. The main techniques are to utilise a **firewall** and to set up some **intrusion detection**.

ICT systems are constantly communicating with the outside world, which involves connection to public networks and the associated difficulty of effectively policing access to the system. A **firewall** is a combination of hardware and software that is designed to check the integrity of incoming messages and requests for service from the system.



Intrusion detection systems (IDS) are designed to monitor the network or computer system for malicious activities. Once an incident is detected, a report is produced which is sent to the network management for further action to prevent any risk to the system.

A computer **virus** is a program designed to cause damage to a computer system. The use of a virus scanner or anti-virus software helps to minimise the risk from viruses; this software searches the computer system for viruses and deletes them once detected.

**Spyware** can be loaded into a computer system as a software virus; it is therefore important to run an anti-spyware program which will prevent and detect spyware from being installed and to remove any spyware that has previously been installed.