Definitions and Concepts for OCR Computer Science GCSE

# Topic 1: Computer systems

## 1.1 – Systems architecture

**Central Processing Unit (CPU):** The hardware component within a computer that carries out the instructions of a computer program.

**Fetch-Execute Cycle:** The fundamental process by which the CPU continually retrieves instructions stored in main memory and executes them.

**Arithmetic Logic Unit (ALU):** A component within the CPU responsible for performing arithmetic operations (addition, subtraction, etc.) and logical operations (AND, OR, NOT).

**Control Unit (CU):** A component within the CPU that manages and coordinates the other components of the computer, fetching and decoding instructions.

**Cache:** A small, fast memory device located on the CPU that stores frequently used data and instructions, providing faster access than main memory.

**Register:** A small, very fast storage location within the CPU that holds data temporarily during processing.

**Von Neumann architecture:** A model for CPU design where both instructions and data are stored in the same memory.

**Memory Address Register (MAR):** A register that stores the address to fetch data from or the address where the data is to be stored.

**Memory Data Register (MDR):** A register that stores the data that is being fetched from or written to memory. It acts as a buffer between main memory and the CPU.

**Program Counter:** A register that stores the address of the next instruction to be fetched from memory. It increments during each fetch-execute cycle to point to the next instruction.

**Accumulator:** A register that stores the results of calculations or operations carried out by the Arithmetic Logic Unit (ALU). Also temporarily holds data being processed.

**Clock Speed:** The rate at which a CPU executes instructions, measured in Hertz (Hz), which affects CPU performance.

**Number of Processor Cores:** The number of independent processing units within a single CPU, allowing for parallel execution of tasks and affecting performance.

**Cache Size:** The amount of fast, temporary memory (cache) available to the CPU, which stores frequently accessed data for quicker retrieval and affects performance.

**Embedded System:** A computer system with a simple, dedicated function within a larger mechanical or electronic system (e.g., in a washing machine or car).

## 1.2 – Memory and storage

**Primary Storage:** The computer's workspace for actively running programs, providing fast access to data and instructions currently in use by the CPU.

**RAM (Random Access Memory):** Volatile main memory that can be read from and written to, used for temporary storage of data and programs currently in use by the CPU.

**ROM (Read-Only Memory):** Non-volatile memory that can only be read from, typically storing essential startup instructions that do not change.

**Volatile:** A type of memory whose contents are lost when the computer loses power.

**Virtual Memory:** A memory management technique that allows a computer to run more programs than it has physical RAM (Random Access Memory) by using a portion of the hard drive as if it were RAM.

**Cache:** Super fast memory located on the CPU. For more information, see 1.1

**Secondary Storage:** Non-volatile storage mechanisms that are not directly accessible by the CPU, used for long-term, persistent storage of data (e.g., hard drives, SSDs).

**Solid State Storage (SSD):** A type of secondary storage that uses electrical circuits (flash memory, specifically NAND gates) to persistently store data, with no moving parts.

**Optical Storage:** A type of secondary storage that uses lasers to read and write data on a rotating disc (e.g., CDs, DVDs, Blu-ray discs).

**Magnetic Storage:** A type of secondary storage that uses magnetic patterns to store data on a rapidly rotating disk (e.g., Hard Disk Drives - HDDs).

**Decimal (Base 10):** A number base using ten unique digits (0-9).

**Binary (Base 2):** A number base using two unique digits (0 and 1), which computers use to represent all data and instructions.

**Hexadecimal (Base 16):** A number base using sixteen unique symbols (0-9 and A-F), often used by programmers for its compact representation of binary data.

**Bit:** The fundamental unit of information, representing either a 0 or a 1.

**Nibble:** A group of 4 bits or half a byte

**Byte:** A group of 8 bits.

**Kilo (kB):** A decimal prefix representing 1,000 bytes.

**Mega (MB):** A decimal prefix representing 1,000 kilobytes (1,000,000 bytes).

**Giga (GB):** A decimal prefix representing 1,000 megabytes (1,000,000,000 bytes).

**Tera (TB):** A decimal prefix representing 1,000 gigabytes (1,000,000,000,000 bytes).

**Petabyte (PB):** A decimal prefix representing 1,000 terabytes

**Binary Shift (Logical):** An operation that moves all bits in a binary number a specified number of positions to the left or right, effectively multiplying or dividing by powers of 2.

**Character Set:** A defined list of characters that a computer can recognise and use, each mapped to a unique, numerical binary code.

**ASCII:** An early character encoding method, primarily used for English text.

**Unicode:** A character encoding standard designed to represent text in all of the world's languages, including non-English alphabets and emojis.

**Pixel:** Short for "picture element," a single point in an image.

**Resolution:** The number of pixels in an image (width x height).

**Colour Depth:** The number of bits used to represent the colour of each pixel in an image.

**Metadata (Images):** Data about an image such as: file format, resolution, colour depth, and sometimes details like the device used to capture the image.

**Analogue Sound:** Sound that is continuous and varying in amplitude and frequency, found in the real world.

**Sample (Sound):** A measure of the amplitude of an analogue sound wave taken at a specific point in time during the digital conversion process.

**Sampling Rate (Sound):** The number of samples taken per second when converting analogue sound to digital, measured in hertz (Hz).

**Bit Depth (Sound):** The number of bits used to store the amplitude of each sample when converting analogue sound to digital.

**Data Compression:** The process of encoding information using fewer bits than the original representation, to save storage space or reduce transmission time.

**Lossy Compression:** A form of compression where some information is lost in the process of reducing the file's size.

**Lossless Compression:** A form of compression where all original information is retained.

## 1.3 – Computer networks, connections and protocols

**Computer Network:** A group of connected devices that can share data and resources.

**Local Area Network (LAN):** A computer network that usually covers a relatively small geographical area, such as a home, school, or office and is often owned and managed by a single person or organisation.

**Wide Area Network (WAN):** A computer network that covers a wide geographic area, connecting multiple LANs, often under collective or distributed ownership (the Internet is the biggest example).

**Bandwidth:** The maximum amount of data that can be transmitted over a network in a given time, usually measured in bits per second (bps). Higher bandwidth allows for faster data transfer.

**Client-Server Network:** A network model where clients (user devices) request resources from servers, which are powerful computers that manage and provide those resources.

**Peer-to-Peer Network:** A network model where all devices (peers) are equal and can both request and provide resources directly to one another, without a central server.

**Wireless Access Point (WAP):** A device that allows wireless-enabled devices to connect to a network using radio waves.

**Router:** A device that connects different networks together and directs data between them - commonly used to connect LANs to the Internet.

**Switch:** A device that connects devices on a LAN and directs data to its correct destination on the network.

**Network Interface Card/Controller (NIC):** Hardware inside a device that allows it to connect to a network by sending and receiving data signals.

**Transmission Media:** The physical or wireless means by which data is transmitted in a network, such as copper cables, fibre optics, or radio waves.

**Internet:** A global network of interconnected computer networks that enables communication and data sharing worldwide.

**Domain Name System (DNS):** A system made up of multiple Domain Name Servers that convert URLs (like www.example.com) into IP addresses that computers use to find and communicate with each other.

**Hosting:** The process of storing website files on a server to make them accessible to a wider audience via the internet.

**The Cloud:** The use of remote servers hosted on the internet to store data and run applications, allowing access from any internet-connected device.

**Web Server:** A computer that stores and serves web pages to clients (e.g., browsers) upon request.

**Client:** A device or program that sends requests to a server and receives responses, such as a web browser.

**Star Topology:** A network layout where each device is connected directly to a central switch, which manages communication between devices.

**Mesh Topology:** A network layout where each device is connected to multiple other devices, allowing data to take the most efficient route to its destination.

**Ethernet:** A common wired networking technology used in LANs for fast and reliable data transmission.

**Wi-Fi:** A wireless technology that uses radio waves to connect devices to a LAN and provide internet access.

**Bluetooth:** A short-range wireless technology used for connecting devices over short distances, typically up to 10 metres.

**Encryption:** The process of converting data into a coded format so that only authorised users with the correct decryption key can read it.

**IP Address:** A unique address used to identify a device on a network. IPv4 uses 32-bit addresses; IPv6 uses 128-bit addresses, allowing for a greater number of unique addresses.

**MAC Address:** A permanent, unique hardware identifier assigned to a device's network interface controller at manufacture, used for communication on local networks.

**Standards:** Agreed rules that ensure compatibility and interoperability between hardware and software from different manufacturers.

**Protocol:** A set of rules that define how data is transmitted across a network.

**TCP/IP (Transmission Control Protocol / Internet Protocol):** A set of protocols used to transfer data over the internet. TCP ensures reliable transmission; IP handles addressing and routing.

**HTTP (Hypertext Transfer Protocol):** An application layer protocol for transferring web pages and other content between web servers and browsers.

**HTTPS (Hypertext Transfer Protocol Secure):** A secure version of HTTP that encrypts communications between a web browser and a website, providing secure web transactions.

**FTP (File Transfer Protocol):** An application layer protocol used for transferring files between a client and a server on a computer network.

**POP (Post Office Protocol):** A protocol that downloads emails from a server to a client and typically deletes them from the server afterward.

**IMAP (Internet Message Access Protocol):** An email protocol used for retrieving and managing email messages directly on a mail server, allowing multiple devices to access the same mailbox. Operates at the application layer.

**SMTP (Simple Mail Transfer Protocol):** An email protocol primarily used for sending outgoing email messages between mail servers and from a client to a server. Operates at the application layer.

**Layers:** A way of organising network communication into separate parts, each handling a specific function and interacting only with adjacent layers.

## 1.4 – Network security

**Malware (Malicious Code):** A general term for harmful software designed to damage, disrupt or gain unauthorised access to computer systems, including viruses, trojans, and spyware.

**Computer Virus:** A type of malware that attaches itself to a legitimate file or program and spreads when the file is opened, potentially corrupting or deleting data or slowing down systems.

**Trojan:** Malicious software disguised as a legitimate program. Once installed, it can allow hackers to access the system, steal data or install more malware.

**Spyware:** A type of malware that secretly collects information about a user's activities, such as keystrokes or login details, and sends it to an attacker.

**Social Engineering:** The manipulation of people into revealing confidential information by exploiting human psychology, rather than using technical hacking methods.

**Phishing:** A form of social engineering where attackers send fake emails or messages pretending to be from trusted sources, tricking users into giving away personal information such as login details.

**Brute-force Attack:** An automated method of trying many different combinations of usernames and passwords until the correct one is found to gain access to an account or system.

**Denial of Service Attack:** An attack that floods a website or online service with excessive traffic, slowing it down or making it completely unavailable to legitimate users.

**Data Interception and Theft:** The unauthorised capturing of data as it is sent over a network, often using special software to listen for unencrypted information such as passwords or credit card numbers.

**SQL Injection:** A technique where an attacker enters specially crafted SQL code into a website input field to gain unauthorised access to or control over a database.

**Penetration Testing:** A method of testing a system's security by simulating an attack to identify vulnerabilities that hackers could exploit.

**Anti-malware Software:** Software that scans files and programs for known malware and removes or blocks them to protect the system.

**Firewall:** A security system that monitors and filters incoming and outgoing network traffic based on a set of security rules, helping to block unauthorised access.

**User Access Levels:** Settings that control what parts of a system different users can access, helping to prevent misuse of data and limit damage if accounts are compromised.

**Passwords:** A security measure used to restrict access to systems or data, requiring users to enter a secret combination of characters to log in. Strong passwords help prevent unauthorised access.

**Physical Security:** The use of physical barriers and controls such as locks, CCTV and security guards to protect computer hardware and data from theft or damage.

## 1.5 – Systems software

**Operating System:** A type of software that manages and controls the computer. It performs essential tasks like managing memory, handling input/output, and providing a user interface.

**User Interface:** The part of the operating system that allows users to interact with the computer. It can be graphical (with icons and menus) or text-based (where commands are typed).

**Memory Management:** The process by which the operating system allocates sections of RAM to different applications, keeps track of memory use, and frees up memory when programs close.

**Multitasking:** The ability of the operating system to run multiple programs at the same time by switching quickly between them and sharing processing time.

**Peripheral Management:** The operating system's job of managing devices connected to the computer, such as keyboards, printers, and monitors, by sending signals and handling data transfer.

**Driver:** A small program used by the operating system to communicate with hardware devices. Each device needs the correct driver to work properly as it acts as a translator between the operating system and the hardware.

**User Management:** The way the operating system creates and controls different user accounts, including managing usernames, passwords, access levels, and keeping user data private.

**File Management:** The organisation and handling of files on a computer. This includes creating, saving, moving, deleting, and naming files, as well as tracking where they are stored.

**Utility Software:** Additional software that performs housekeeping tasks to help maintain or improve the system. Examples include encryption software, defragmentation software, and data compression software.

**Encryption Software:** Software that scrambles data into a coded format so it can only be understood by someone with the correct decryption key, helping to keep data secure.

**Defragmentation Software:** Software that reorganises files on a hard disk so that they take up fewer separate spaces, improving system speed and performance.

**Data Compression Software:** Software that reduces the size of files so they take up less storage space and can be transferred over a network more quickly.

## 1.6 – Ethical, legal, cultural and environmental impacts of digital technology

**Ethical Issues:** Questions about what is morally and ethically right or wrong in the use of technology. These issues are wide-ranging and subjective, and there isn't necessarily a correct answer to solving them.

**Legal Issues:** Issues relating to whether computing technology is legal under the current legislation.

**Cultural Issues:** Issues that arise from differences in moral values and the use of technology based on people's traditions and beliefs.

**Environmental Issues:** The impact that computers and digital technology have on the natural world, such as energy usage, use of limited resources, and e-waste.

**Data Privacy:** The right of individuals to control how their personal information is collected, stored, used, and shared and the measures taken to protect this information from unauthorised access.

**Data Protection Act 2018:** A UK law that governs how organisations use personal data. Personal data must be used lawfully, stored securely, kept accurate, and not kept longer than necessary. People have rights such as:

- The right to be informed about how data is used
- The right to access or erase their data
- The right to stop data being processed

**Computer Misuse Act 1990:** A UK law that prevents unauthorised access or damage to computer systems. Offences include:

- Unauthorised access to computer material
- Access with intent to commit further crimes
- Acts intended to impair computer operations
- Acts causing serious damage
- Making or distributing hacking tools

**Copyright, Designs and Patents Act 1988:** A UK law that protects original works like music, books, software and images from being copied or used without permission. The creator automatically owns the copyright and can decide how their work is used.

**Open Source Software:** Software made freely available for anyone to use, modify and distribute.

**Proprietary Software:** Software owned by a company with source code kept secret. Users must buy a licence and cannot modify it.