KS4 Computer Science Knowledge Organiser

Contents

Computer Hardware – Key Terms

Key Term	Definition
Hardware	The physical parts or components of the computer
Peripheral	A device attached to and under the control of the computer
Input peripheral	Used to bring data from the physical world into the computer
Output peripheral	Used to transfer information from the computer to the physical world
Storage peripheral	Device used to store data and files.
CPU	Central Processing Unit. Executes commands and controls the computer.
Motherboard	Connects all the hardware components and allows them to communicate.

Key Term	Definition
RAM	Random Access Memory. Volatile. Instructions and data stored here.
Hard drive	Long term storage device. Non-volatile. Information stored magnetically.
SSD drive	Alternative to Hard drive. Less capacity but faster and more robust.
Optical drive	Blu-ray, DVD, CD. Lasers used to store and read information. Pits and lands.
Graphics Card	Executes the graphics instructions. GPU – Graphics Processing Unit.
PSU	Power Supply Unit. Supplies power to all the components of the computer.
BIOS	Basic Input Output System. Loads the operating system upon startup.

Memory

Key Term	Definition
Primary Memory	Memory used to store data and instructions that are required by the CPU.
RAM	Random Access Memory is volatile memory used to store data and instructions which are needed by the CPU. Also referred to as main memory.
Dynamic RAM	Contains 1 transistor and capacitor that hold charge briefly. This needs to be refreshed every few milliseconds.
Static RAM	Uses 5 transistors which are wired together to represent each bit. No need to be refreshed. More wiring per bit.
ROM	Read only memory. Used to store the boot sequence as this should never be changed. This memory is non-volatile

Key Term	Definition
Bootstrap loader	A small program that loads the operating system. Once the operating system is loaded it takes care of the rest.
Flash Memory	Electrons are forced into a layer between two barriers which hold the charge by using a high electric current.
Virtual Memory	When RAM is full, a section of the hard drive can be used to store programs and instructions.
Volatile	Storage which needs to have power to store data. If power is lost, data is lost.
Non-Volatile	Storage which does not lose its contents when the power is lost.

Threats

Key Term	Definition
Blagging	Knowingly or recklessly obtaining or disclosing personal data or information without the consent of the controller (Owner of data). EG Employees sharing passwords.
Hacking	Attempting to gain access to a system through cracking passwords.
Human Error	People are often the weakest part of security systems and criminals take advantage of human error and gullibility.
Malware	Software that can harm devices, which is installed on someone's device without their knowledge or consent. May be spread by email, messaging services or downloading infected files.
Phishing	Emails designed to appear as a reputable organisation to gain trust of users and harvest personal information.
Spyware	Secretly monitors user actions (eg. key presses) and sends info to a hacker.

Key Terms	Definitions
Poor Network Policies	Network policies are not always designed to provide maximum security. For example, a strong policy should recommend changing passwords regularly and ensure that the passwords used meet the strength and history requirements.
SQL Injection	Technique that exploits security weaknesses in websites. Achieved by inserting malicious code into a database field on a website such as a password field.
Trojan	Trojans are malware disguised as legitimate software. Unlike viruses and worms, Trojans do not replicate themselves – users install them not realising they have a hidden purpose.
Virus	Viruses attach (by copying themselves) to certain files. Users spread them by copying infected files and activate them by opening those files.
Worm	Worms are like viruses but they self-replicate without any user help, meaning they can spread very quickly.

Hacking

Key Term	Definition
Active	When someone attacks a network, for example with malware.
Brute force	A type of active attack used to gain information by cracking passwords through ‘trial and error’. Uses likely password combinations to gain access to user accounts.
Data Interception and Theft	Measures to reduce this risk include destroying paper documents when no longer needed, logging off or locking computers when not in use and locking rooms containing computers.
Denial-of-se rvice	Where a hacker tries to stop users from accessing a part of a network or website, mostly by flooding the network with useless requests, making the network very slow or completely inaccessible.

Key Term	Definition
Insider	When someone within an organisation exploits their network access to steal information.
Passive	Where someone monitors data travelling on a network and intercepts any sensitive information they find.
Shouldering	Attempting to look over someone’s shoulder when using an ATM.

Prevention

Key Term	Definition
Access Levels	Allows a system administrator to set up a hierarchy of users. Low-level users can access only a limited set of information.
Antimalware	Preventing installation of harmful software, preventing important files from being changed, scanning for virus activity on the system and removing as appropriate. Antimalware protects against worms, trojan horses, spyware, adware and key-loggers.
Antivirus	Software designed to protect against viruses.
Encryption - Symmetric	Cryptographic algorithm that uses the same key to encrypt and decrypt the data.

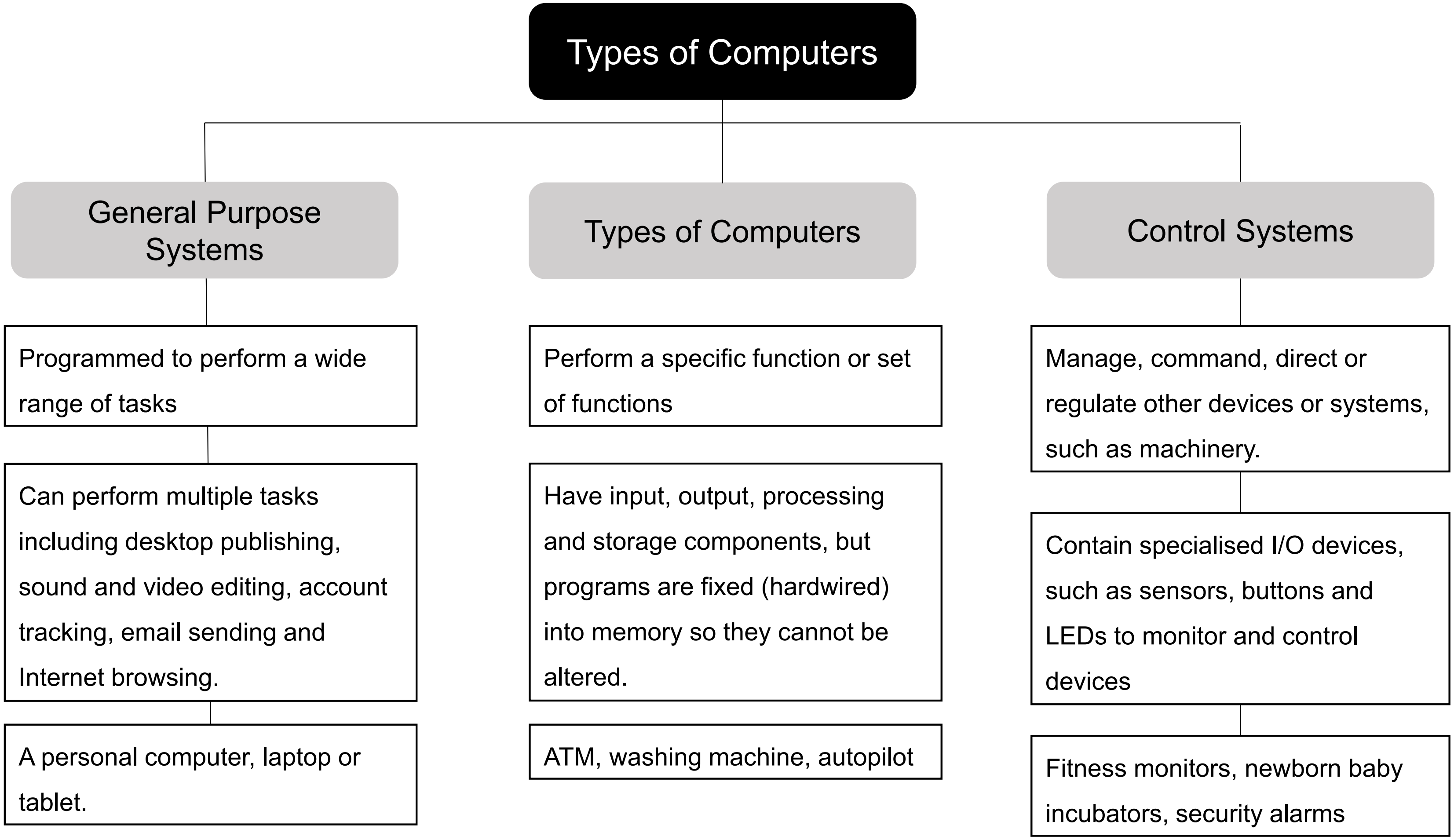
Key Term	Definition
Encryption - Asymmetric	Asymmetric cryptography, also known as public key cryptography, uses pairs of public and private keys to encrypt and decrypt data. A message encrypted with a public key can only be decrypted with its paired private key.
Firewall	Hardware or software designed to prevent unauthorised access to or from a private network or intranet. All messages entering or leaving the network will pass through the firewall to be examined.
Password Protection	Passwords should be strong – length, upper & lower case, numbers and special characters and should also meet the history requirement – they should not have been used before.

System Software

Key Term	Definition
User Interface	The means by which the user and a computer system interact, in particular the use of input devices and software.
Memory Management	The process of controlling and allocating the available computer memory to all the running processes that need it.
Multi-Tasking	Performing multiple tasks (also known as processes) over a certain period of time by executing them concurrently.
User Management	Allowing different types of users to login and access information relevant to their job.
Peripheral Management	Controls peripheral devices by sending them commands in their own computer language
File Management	Manages the file hierarchy and the data files in a computer system

Key Term	**Definition**
Encryption software	Uses cryptography to prevent unauthorised access to digital information
Defragmentation	Process of locating the non-contiguous fragments of data into which a computer file may be divided as it is stored on a hard disk
Data Compression	Compression can be either lossy or lossless. Lossless compression reduces bits by identifying and eliminating statistical redundancy.
Full Backup	A backup of the entire computer system. Contains all the data in the folders and files that are selected to be backed up.
Incremental Backup	Contains only those files which have been altered since the last full backup

Types of Computers



Types of Computers

General Purpose Systems

Programmed to perform a wide range of tasks

Can perform multiple tasks including desktop publishing, sound and video editing, account tracking, email sending and Internet browsing.

A personal computer, laptop or tablet.

Types of Computers

Perform a specific function or set of functions

Have input, output, processing and storage components, but programs are fixed (hardwired) into memory so they cannot be altered.

ATM, washing machine, autopilot

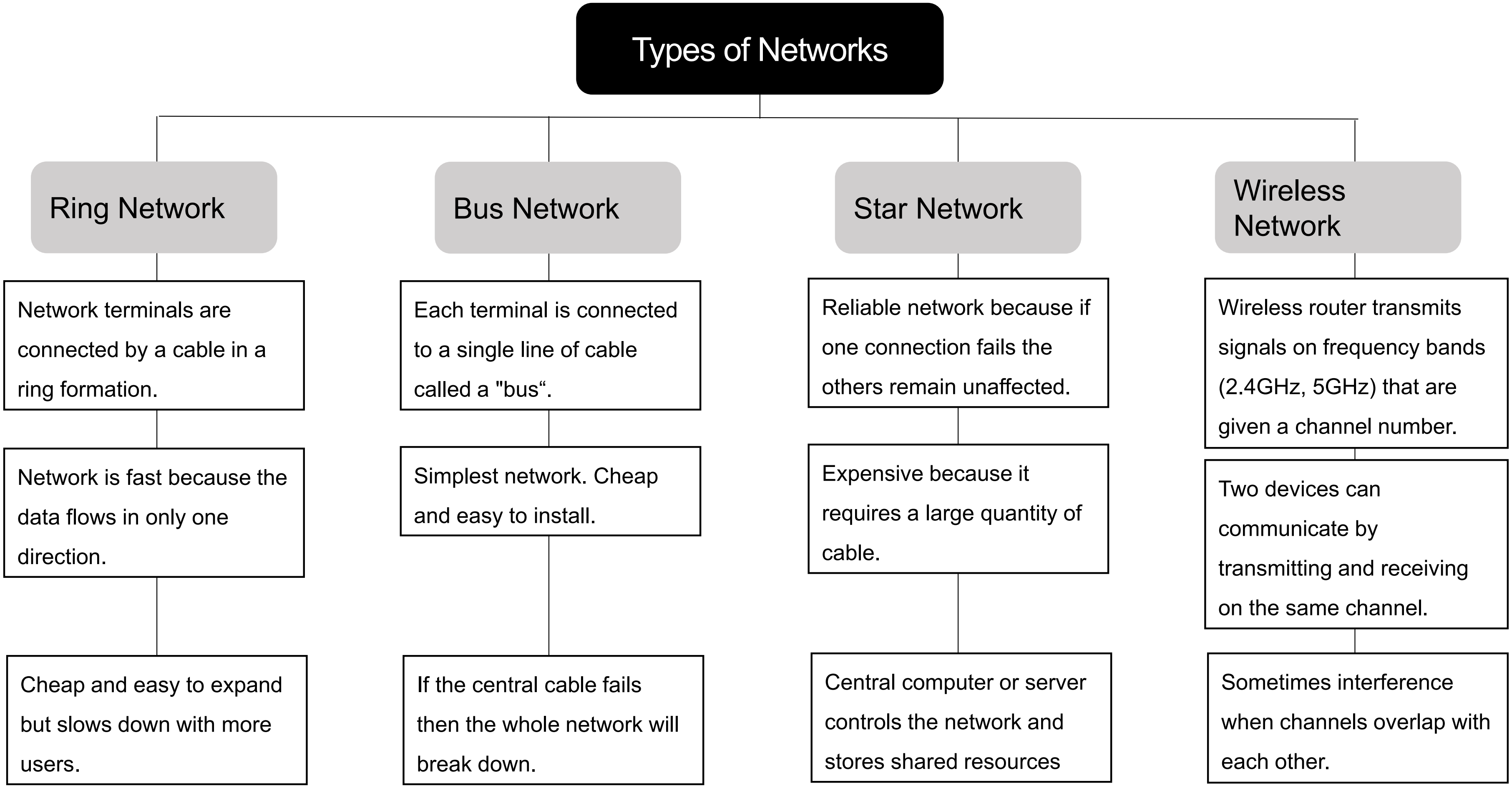
Control Systems

Manage, command, direct or regulate other devices or systems, such as machinery.

Contain specialised I/O devices, such as sensors, buttons and LEDs to monitor and control devices

Fitness monitors, newborn baby incubators, security alarms

Types of Networks



Types of Networks

Ring Network

Network terminals are connected by a cable in a ring formation.

Network is fast because the data flows in only one direction.

Cheap and easy to expand but slows down with more users.

Bus Network

Each terminal is connected to a single line of cable called a "bus“.

Simplest network. Cheap and easy to install.

If the central cable fails then the whole network will break down.

Star Network

Reliable network because if one connection fails the others remain unaffected.

Expensive because it requires a large quantity of cable.

Central computer or server controls the network and stores shared resources

Wireless Network

Wireless router transmits signals on frequency bands (2.4GHz, 5GHz) that are given a channel number.

Two devices can communicate by transmitting and receiving on the same channel.

Sometimes interference when channels overlap with each other.