Data that is currently being processed is held in memory. Memory chips are either in RAM or ROM format.

RAM stands for Random Access Memory, volatile memory or memory that loses its contents when the power is off. Volatile means it can be erased or closed out of easily.

ROM stands for Read Only Memory. ROM is non-volatile and does not lose its contents when the power is off. Non-volatile means it can not be erased or closed out of easily.

Backing storage holds the data that the computer does not currently need but may draw from when needed.

Backing storage may be either magnetic (uses polar energy), such as a magnetic or cassette tape, or optical (uses a light sensor) such as a compact disc (CD).

Magnetic tapes are old but still used for backing up data. They only allow sequential storage (one data item after another, in the order they arrive) and are often slow.

Hard discs (CD's) contain more, spin all the time (faster access) and are the main backing storage for most computers. Disc storage allows either direct (jump straight to a track) or sequential access.

CD storage is suitable for reference material and software installations. CD-ROM's cannot be altered, CD-R's can be used once to store data, CD-RW's several times. DVD storage is suitable for video, large books and very large amounts of data and back-up.

Flash memory (a form of non-volatile RAM) is becoming popular rapidly because it is small, portable, inexpensive and easy to manage. An example of Flash memory is a USB device.

A backup is a copy of data stored in a different place. Three examples of cataclysms that may cause data loss or damage are fire, flood or theft.

Vocabulary Focus:

ROM  non-volatile memory type, the contents are not erased easily
volatile means it can be erased or closed out of easily
magnetic tape magnetic backing storage; allows sequential storage (one data term after another), often slow.
RAM volatile memory type that can be erased easily
USB drive small, portable, inexpensive device used in Flash memory
backup copy of data stored in a different place
magnetic backup storage that uses polar energy
optical backup storage that uses a light sensor
Flash memory non-volatile RAM, backing storage in small, portable devices
magnetic disc removable magnetic storage, allows for skip storage, fast access
non-volatile means it can not be erased or closed out of easily
Storage Devices and Media: The Importance Data Backup, Practical Uses and Applications

Data storage capacity - Refer to the chart for storage devices and their capacities

Storage is measured in bytes (B). A byte is a unit of data, eight binary (0's and 1's) digits long. Most computers use bytes to represent a character such as a letter, number, or typographic symbol (such as "g", "5", or ").

A byte can also hold information to be used in some larger unit for application purposes (for example, making a visual image for a program that displays images or the machine code of a computer program).

<table>
<thead>
<tr>
<th>Type</th>
<th>Abbreviation</th>
<th>Amount equal to</th>
<th>Therefore...</th>
</tr>
</thead>
<tbody>
<tr>
<td>kilobyte</td>
<td>KB</td>
<td>one thousand bytes</td>
<td>1,000B = 1KB</td>
</tr>
<tr>
<td>megabyte</td>
<td>MB</td>
<td>one million bytes</td>
<td>1,000,000B = 1MB</td>
</tr>
<tr>
<td>gigabyte</td>
<td>GB</td>
<td>one thousand million bytes</td>
<td>1,000,000,000B = 1GB</td>
</tr>
<tr>
<td>terabyte</td>
<td>TB</td>
<td>one million million bytes</td>
<td>1,000,000,000,000B = 1TB</td>
</tr>
</tbody>
</table>

The Importance of Data Backup

Backing up data means making an extra copy of computer information so that if, in the event of a problem, loss of the original file, or damage to the computer, the backup copy can be used as a replacement.

Corrupted files are data or program files that have been altered accidentally by hardware or software failure. Corruption of the file causes the bits to be rearranged and renders it either unreadable to the hardware or, if readable, indecipherable to the program.

Off-Site Backup means making duplicate copies of files to store in a different geographic location such as in another building or at a cloud storage facility on the Internet. Also called "off-site data protection" or "vaulting." off-site backup is required for disaster recovery, and to prevent damage from viruses such as on a local network.

Are you backing up data? – 4 important questions – remember the SAUCE!

Speed – how fast will the back up take to do? How fast can I retrieve what I need?
Access – how easy is the information to find? Who will have access to the files?
Use – how easy is the back up device (or software) to use?
Cost – what is the price of the back up? Is it practical for the task I need?
ICT Storage Devices and Media Study Guide
Includes RAM, ROM, devices, bits, bytes, floppy disks, malware and viruses

Learn about Floppy Disks, Bits, Bytes, Kilobytes (KB), Megabytes (MB), Gigabytes (GB), Terabytes (TB).
From the video by Dane Hartman on YouTube https://www.youtube.com/watch?v=HRmfXA4EUBs

FIRST, THERE WERE FLOPPY DISKS!

Do you know your Floppy Disks?

<table>
<thead>
<tr>
<th>Floppy Disk</th>
<th>Format</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 inch</td>
<td>1960s-70s</td>
<td>about 80 KB</td>
</tr>
<tr>
<td>5.25 inch</td>
<td>1970s-80s</td>
<td>about 360 KB</td>
</tr>
<tr>
<td>3.5 inch</td>
<td>1980s</td>
<td>about 144 MB</td>
</tr>
</tbody>
</table>

Computers use the Binary number system, which has only two numbers, one and zero. These binary digits, which can be either one or zero, is Bit – B-I-T, short for ‘binary digit.’ A bit is the smallest unit of data in a computer. Bits are used to store information, from the text that appears on your screen, to the colors of an image, to the sounds that come out of your speakers. To store information like this, we use many bits together.

The number of bits a user has determines how much information can be stored on a device, such as a disk.

If you take 8 of these bits – 8 of these ones and zeroes - and put them together, that’s called a Byte. A Byte is 8 bits put together; one byte represents the amount of space it takes to store one single letter or symbol in a text document. If you wrote a short story with 1000 words, this would take up 1000 bytes of storage space.

1000 bytes put them together is called a Kilobyte, abbreviated as KB. There are actually 1024 bytes in a kilobyte, because computers use binary and everything comes in powers of two. Think of a kilobyte simply as 1000 bytes, like a kilometer is 1000 meters.

One of the first portable storage devices, the 8 inch floppy, was not re-writeable and held only 80 KB of memory.

One Kilobyte is enough space to hold about two pages of text. Back in the late 1970s and early 1980s, the 5.25” floppy disk, a popular storage option, could hold 360kb of information.

1000 kilobytes equal a Megabyte, abbreviated as “MB”. One megabyte is enough space to hold about 5 books, or one photo, or one minute of music. Back in the mid-1980s, a 3.5” floppy disk, held 1.44MB of data, which was pretty good at the time, because most files were pretty small.

1000 megabytes equal a Gigabyte, abbreviated as GB. A GB holds about 400 books, or 1,000 pictures, or 16 hours of music. By the mid 1990s, you could buy a 1GB hard drive for a couple hundred bucks. Today, you can buy 1 GB flash drive for about $5.

1000 gigabytes equal a Terabyte, abbreviated as “TB.” A TB holds about 400,000 books (about 30 libraries), a million pictures, or two years of continuous music. Today, you can buy a 1TB hard drive for under $50.
Cloning Vs. Imaging

Cloning and Imaging are two ways that information can be backed up and saved from a computer. These methods are generally used by large corporations with extensive amounts of data, or individuals needing an exact copy of another computer and all its files.

To clone a drive, you copy everything on it onto another drive, so that the two are effectively identical. Normally, you would clone to an internal drive by connecting to it with a special adapter.

In this clone diagram, one computer is used as the master. The information on the master is transferred to a computer that holds the data in a shared folder. The data is then sent to several others computers exactly as it is contained in the master computer.

To image a drive, you gather all the information like a great big .zip file (without the .zip extension), including the software and technology already on the computer, to aid you in the imaging process. The image is an exact replica of your computer at the time the information was taken. Image backup software copies everything on the drive into a single, compressed, but still very large file. You would probably then save the image onto an external hard drive. Imaging is generally done through a software program.

In this image diagram, one computer is used as the master. The information on the master is transferred from one computer to the other, so that both computers look exactly the same once the process is finished.

Which process would be more effective for someone who has purchased a new computer? Why?

Which process would be more effective in a school for students in a classroom setting? Why?
Malware and Other Issues with Information Found on the Internet

Try to keep Cloning and Imaging safe from Malware and viruses when transferring files or complete drives. 'Malware' refers to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan Horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.

**Ransomware** - a type of malware that prevents or limits users from accessing their system and forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back.

**Spyware** - software that enables a user to spy on and obtain covert information about another’s computer activities by transmitting data covertly from their hard drive.

**Adware** - advertising-supported software. A software package that automatically renders advertisements in order to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process.

**Scareware** - tricks victims into purchasing and downloading useless and potentially dangerous software by generating pop-ups that resemble Windows system messages, usually posing as antivirus software, a firewall application or a registry cleaner to scare users into thinking they need the product.

**Hacking** – the process of accessing a computer system without permission. Performed by hackers, people who try to guess passwords and break codes to access personal data. Hacking may be done through email or database servers, or using any of hundreds of computer-based external devices to assist in the chosen method of extracting encrypted information.

**extracting** (extracted) – removing or excerpting  
**encrypted** – set in code or a secret language

**Phishing** – fraudulently trying to get users to reveal user names, passwords, credit card details or other account information by posing as a financial institution or other legitimate company, generally contacting the user by email.

**Smishing** – similar to phishing except the messages are sent to you via SMS Text versus email message. The link is sent in a message which is clickable or copyable; it usually leads to a bogus website requesting your bank or other personal information. Smishing has become increasingly popular as people move away from having landlines in their home, with the cellphone as their only means of phone communication.

**Pharming** – malicious programming code stored on a computer, where any users who try to access a website stored on the computer will be automatically redirected to a bogus website website that mimics the appearance of a legitimate one, not actually the site they wanted.

**Spam** – unwanted email sent automatically and indiscriminately (lacking in care) to multiple recipients, usually advertising or requesting action from the user. Also called junk mail, spam is not illegal in most countries! Filters may be set up to try to prevent or remove spam from being received in your email in box.
Viruses, Worms, Trojan Horses and Hoaxes


Virus – a program that attaches itself to other programs or files, designed to be able to copy itself

• A virus tries to spread from one computer to another
• A virus can only spread through the actions of the user
• A virus will not send itself; it infects files, and those files are then forwarded, or passed on
• A virus goes to work when an infected file is opened
• The damage from a virus can vary from slightly annoying side effects (slow computer, windows popping up, change in the PC’s behavior, etc.) to full destruction (erasing files or the hard drive)
• A virus can cause damage to software or to the information held in files

Worm – a computer-infecting program or code that is spread from one machine to another

• A worm does not rely on the actions of the user: a worm can spread automatically
• A worm does not have to attach itself to other files; it is able to spread independently by a mechanism incorporated in the worm
• Worms try to guide an infected code through a door to a computer, like an Internet connection
• Worms can spread through emails of the address book or webmail of the infected computer
• The first thing a worm does is cause an increase in network traffic
• The worm makes normal programs run slowly, stop altogether or steal users’ personal info

Trojan Horse – a poisoned piece of software attached to a program that was installed by a user.

• At first, a Trojan Horse looks like a useful program
• A Trojan Horse causes damage to computer data or gathers the user’s private information
• A Trojan Horse spreads via the Internet or as an attachment to an email that looks reliable
• A Trojan Horse can be downloaded (“Download this program, make your PC times faster!”)
• Trojan Horses do not copy themselves independently to other computers.
• Trojan Horses can take over your computer, discover passwords, share, change or delete files, turn your computer into a bot (sending Trojan Horses to other), and totally crash your computer

Hoax – not a virus, but rather a false virus warning that can steal some personal information

• A hoax may appear as a warning about a “new virus” in your mailbox, or a chain email story
• Hoaxes are usually designed to generate fear or sympathy, and are thus spread to lots of people
• Hoaxes urge you immediately send the email on to everyone else in your address book
• With hoaxes, spammers get hold of stacks of email addresses through the false warnings sent out

3 Easy Way to Protect your Computer – Source: https://youtu.be/uJRqZTNMCMo

1. Update your operating system
2. Don't click on unknown links and
3. Use caution when attaching items to email