POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Digitally Stored Evidence

Standard Operating Procedure

Notice:

This document has been made available through the Police Service of Scotland Freedom of Information Publication Scheme. It should not be utilised as guidance or instruction by any police officer or employee as it may have been redacted due to legal exemptions

Owning Department:	Specialist Crime Division
Version Number:	2.00
Date Published:	16/03/2018

Compliance Record

Equality and Human Rights Impact Assessment (EqHRIA): Date Completed / Reviewed:	20/03/2017
Information Management Compliant:	Yes
Health and Safety Compliant:	Yes
Publication Scheme Compliant:	No

Version Control Table

Version	History of Amendments	Approval Date
1.00	Initial Approved Version	19/03/2013
2.00	SOP re-formatted to new template and aligned to Corporate identity. Full review conducted with the inclusion of guidance for the Management of Digital Images and amended to reflect recent legislative changes in case law in respect of the examinations of mobile phones in certain circumstance	06/02/2018

Contents

Appendices

1. Purpose

1.1 This Standard Operating Procedure (SOP) supports the Police Service of Scotland, hereafter referred to as Police Scotland, Policies for –

- Crime Investigation Policy
- Records Management Policy

1.2 This Standard Operating Procedure (SOP) provides instruction and guidance to police officers and police staff when dealing with potential evidence stored on digital media devices.

1.3 The rules of evidence apply equally to digital based electronic evidence as much as they do to material obtained from other sources. It is always the responsibility of the officer in charge of a case to ensure compliance with legislation and in particular; to be sure that the procedures adopted in the seizure of any property is done in accordance with statute and current case law.

1.4 The instruction and guidance herein is founded on the ACPO Good Practice Guide for Computer Based Electronic Evidence which was written in association with the Association of Chief Police Officers Scotland (ACPOS). The ACPO Guidance has not been replicated in full; therefore officers may wish refer to the wider guidance provided therein. This guidance remains best practice in respect of electronic evidence.

2. Principles of Digital / Computer Based Evidence

2.1 Four principles are involved:

(a) **Principle 1**: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

(b) **Principle 2**: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

(c) **Principle 3**: An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

(d) **Principle 4**: The officer in charge of the investigation (the OIC) has overall responsibility for ensuring that the law and these principles are adhered to.

2.2 Explanation of the Principles

(a) All digital Evidence is subject to the same rules and laws that apply to documentary evidence.

(b) The doctrine of documentary evidence may be explained thus: the onus is on the prosecution to show to the court that the evidence produced is no more and no less now than when it was first taken into the possession of police.

(c) Operating systems and other programs frequently alter and add to the contents of electronic storage. This may happen automatically without the user necessarily being aware that the data has been changed.

(d) In order to comply with the principles of computer based electronic evidence, wherever practicable, an image should be made of the entire target device. Partial or selective file copying may be considered as an alternative in certain circumstances e.g. when the amount of data to be imaged makes this impracticable.

(e) In a minority of cases, it may not be possible to obtain an image using a recognised imaging device. In these circumstances, it may become necessary for the original machine to be accessed to recover the evidence. With this in mind, it is essential that a witness, who is competent to give evidence to a court of law, makes any such access.

(f) In cases dealing with data which is not stored locally but is stored at a remote, possibly inaccessible location it may not be possible to obtain an image. It may become necessary for the original data to be directly accessed to recover the data. With this in mind. It is essential that a person who is competent to retrieve the data and then be able to give evidence to a court of law makes any such access. Due consideration must also be given to application legislation if data is retrieved which resides in another jurisdiction.

(g) It is essential to display objectivity to a court, as well as the continuity and integrity of evidence. It is also necessary to demonstrate how evidence has been recovered showing each process through which the evidence was obtained. Evidence should be preserved to such an extent that a third party is able to repeat the same process and arrive at the same result as that presented to a court.

(h) It should be noted that the application of the principles does not preclude a proportionate approach to the examination of digital devices. Those making decisions about the conduct of a digital investigation must often make judgements about the focus and scope of an investigation, taking into account available intelligence and investigative resources. This will often include a risk assessment based on technical and non-technical factors, for example the potential evidence which may be held by a particular type of device or the previous offending history of the suspect. Where this is done it should be transparent and decisions made should be justifiable with the rationale recorded.

3. Evidence at Crime Scenes

3.1 The proliferation of digital devices and the advances in digital communications mean that digital evidence is now present or potentially present in almost every crime.

3.2 Digital evidence and associated Communication's Data can be found in a number of different locations:

- Locally on an end-user device – typically a user's computer, mobile/smart phone, satellite navigation system, USB thumb drive or digital camera;
- On a remote resource that is public – for example websites used for social networking, discussion forums and newsgroups;
- On a remote resource that is private – an Internet Service Provider's logs of users' activity, a mobile phone company's records of customers' billing, a user's web mail account, and increasingly common, a user's remote file storage;
- In transit – for example mobile phone text messages, or voice calls, emails, or internet chat.

3.3 These types of digital media and end-user devices all have the potential to hold data which may be of value to the investigation. In order to preserve the data and achieve best evidence, these items must be handled and seized appropriately, and should be treated with as much care as any other item that is to be forensically examined.

3.4 Internet adoption has raised the issue of live examinations where an offender is discovered on line upon warrant execution. Immediate advice should be sought form your local Cybercrime Unit to progress search without loss of crucial evidence.

4. Seizure of Digital Devices

4.1 The following general principles, if adhered to, will ensure the best chance of evidence being recovered in an uncontaminated and therefore acceptable manner:

Desktop and Laptop Computers

- Secure and take control of the area containing the equipment;
- Allow any printers to finish printing;
- Move people away from any computers and power supplies;
- Don't switch the computer on;
- Be aware that some laptop computers may power on by opening the lid;

- It is considered to be best practice to photograph (or video) all the components in situ and if no camera is available, draw a sketch plan of the system;
- Unplug the power from the rear of the system unit (or Laptop) and other devices e.g. printers, by pulling the plug at the back of each unit, not at the wall socket. This is in case a system has an uninterruptible power supply connected. A computer that is apparently switched off may be in sleep mode and may be accessed remotely, allowing the alteration or deletion of files;
- Remove the battery form Laptop Computers;
- If the computer is believed to be networked, seek advice from the Cybercrime Unit;
- Remove all other connection cables leading from the computer to other wall or floor sockets or devices;
- Ensure that all items have signed production labels attached to them, or that they are within the appropriate evidence bags, as failure to do so may create difficulties with continuity and cause the equipment to be rejected by the forensic examiners;
- Search area for diaries, notebooks or pieces of paper with passwords on which are often stuck to or close to the computer;
- Make detailed notes of all actions taken in relation to the computer equipment;
- Where a device is found to be operating with data displayed on a monitor or screen record what is on the screen by photograph or video and by making a written note of the content of the screen;
- Do not touch the keyboard or click the mouse and if the screen is blank or a screen saver is present, the case officer should be asked to decide if they wish to restore the screen. If so, a short movement of the mouse will restore the screen or reveal that the screen saver is password protected. If the screen restores, photograph or video and note its content. If password protection is shown, continue as below without any further touching of the mouse. Record the time and activity of the use of the mouse in these circumstances.

Devices to be seized for the retrieval of Evidence

- All system units and Laptop computers;
- Loose Hard disks (not fitted inside the computer);
- External Drives, including powered drives contained in caddies, USB Pen Drives and other external devices;
- Modems;
- Routers;
- Digital cameras and associated storage media (flash cards, smart media etc.);

- Floppy disks;
- Digital Tape;
- CDs;
- DVDs;
- PCMCIA cards (see glossary);
- MP3 Players;
- Apple mobile devices (iPods, iPads etc.);
- Gaming Machines;
- Electronic Organisers and Personal Digital Assistants (PDAs);
- Mobile Phones including smart phones.

4.2 This is not an exhaustive list and as a general rule if a device is suspected of containing digital evidence, that is

- attributable to the suspect/accused;
- used by the suspect/accused;
- relevant to the crime or enquiry under investigation.

4.3 It should be seized and presented to the Cybercrime Unit for identification and examination. In the larger and more complicated investigations, it is deemed good practice for the Enquiry or Investigating Officer to ensure contact is made with the allocated Forensic Computer Analyst to discuss the case forensic examination

4.4 All officers and members of police staff involved in search duties should be aware that IT competent offenders may endeavor to conceal their devices in obscure places within their homes.

5. Mobile Phones

5.1 The improvements in technology have made mobile telephone examination a complicated process. Some mobile telephones can store names, numbers and text messages in more than one place. Most phones can now store photographs video clips and other data files. Mobile devices can be used to access the Internet, including access to emails and social networking. Many mobile device applications store GPS information that may be relevant to a case.

5.2 Officers seizing mobile telephones during house searches etc. should where possible also take possession of mobile telephone chargers. The owner should be asked to provide the telephone number. This number should be noted, and included on examination request from.

5.3 Non Cybercrime Investigation Examination

5.3.1 A mobile telephone should not be examined by any person connected with the case.

5.3.2 Carrying out an "unofficial" examination may change the contents. The practice of dialling a known telephone number to quickly obtain the telephone number of the mobile phone is not to be carried out. These changes are irreversible and will be identified during the subsequent examination.

5.3.3 Making such changes to a phone's contents after it has been seized as a production may render all the evidence from its contents as being inadmissible in Court.

5.3.4 Recent stated case law and operational scenarios have highlighted opportunities that may exist to expedite urgent enquiries with the manual examination of a mobile phone out with normal submission to your local Cybercrime Forensic Gateway for examination.

5.3.5 On **all** occasions a supervisor of **at least** the rank of Inspector and **not** involved with the case should be contacted and asked for permission to examine the phone.

5.3.6 For the sake of clarity, a manual examination by a police officer involves viewing the live data e.g. text messages, images, etc., held on a mobile telephone (versus a forensic examination that could potentially recover all data.

5.3.7 You may however consider the manual examination of a mobile phone or other mobile device in the following circumstances:-

- Suspect arrested on under the terms of Section 1 of the Criminal Justice (Scotland) Act 2016;
- Suspect detained under the terms of Section 23, Misuse of Drugs Act 1971 **and only when drug dealing is suspected***;*
- Suspect phoned seized under common law and urgency of circumstances dictates that the phone is examined e.g. threat to life;
- Victim hands over phone to officers to examine – often for low-level offences and enables officers to note content of text messages and/or to enable screenshots to be emailed to Police thereby allowing victim to retain phone.

5.3.8 Where a mobile telephone is believed to have been used in the commission of a crime or has been stolen, officers should be aware, in the first instance of the guidance and advice contained in the:

- Cybercrime First Responders Guide;
- Seizure And Forensic Examination Of Mobile Phone;
- Mobile Phone Crime Toolkit.

and also from their local Cybercrime Unit to assist in any investigation.

5.4 Seizure, Labeling and Storage of Mobile Devices

5.4.1 Mobile devices should be switched off and placed in an appropriate container such as a production tube or box.

6. Other Storage Media

6.1 It should be borne in mind that a number of electronic devices encountered at searches might contain evidence relevant to your criminal investigation. These might include:

- Pagers;
- Land line telephones;
- Answering machines;
- Facsimile machines;
- Dictating machines;
- Telephone e-mailers.

6.2 If any of these items are to be seized and disconnected from a power supply, their memory may be erased. Consider consulting the Cybercrime Unit prior to seizing such items.

7. Handling and Transportation

7.1 As a general rule all devices capable of storing digital evidence should be kept away from magnetic sources (loudspeakers, heated seats and windows and police radios). Otherwise digital devices should be afforded the same care and consideration as any other productions seized.

7.2 All officers should consider the manual handling implications when seizing or removing the range of devices that may include large servers or bulky digital equipment. Refer to the Digital Forensic Examination Risk Assessment.

7.3 Preservation of Equipment for DNA or Fingerprint Examination

7.3.1 Where it is likely that digital devices will be required to be examined for fingerprints or DNA they should be seized and stored appropriately, however it should be borne in mind that using aluminium powder on electronic devices can be dangerous and result in the loss of evidence.

7.4 Storage after Seizure

7.4.1 The computer equipment should be stored at normal room temperature without being subject to any extremes of humidity and free from magnetic influence such as radio receivers. Some computers are capable of storing internal data by use of batteries. If the battery is allowed to become flat, internal data will be

lost. Dust, smoke, sand, water and oil are harmful to computers. Aluminium fingerprint powder is especially harmful and dangerous.

7.4.2 For further guidance refer to the Productions SOP.

8. Internet and Social Media Related Crimes

8.1 The primary source of intelligence and evidence regarding the investigation of on-line crimes may lie with the service providers and on seized devices. However, depending on the particular circumstances of the case it may be possible to recover relevant data from digital investigations and as such the opportunities and possibilities should also be discussed with the Internet Investigations Unit or CycComms Unit.

8.2 For specific advice and direction regarding the investigation of Internet and Social Media Related Crimes please refer to the Internet, Research and Investigations SOP.

9. Investigations

9.1 Whenever possible and practicable, thought must be given to the possibility of there being digital / computer based evidence on premises prior to a search being conducted.

9.2 In Scotland, when seeking a search warrant through the relevant Procurator Fiscal, the warrant application should clearly indicate what electronic evidence is anticipated and which persons are required to expedite the recovery and seizure of that material.

9.3 A list of common terms that investigating officers may encounter have been produced in Appendix ‘B’.

9.4 Pre – Search

(a) When a search is to be conducted and where computer based electronic evidence may be encountered, preliminary planning is essential. As much information as possible should be obtained beforehand about the type, location and connection of any computer systems. If medium or large network systems are involved and are considered a vital part of the operation, then relevant expert advice should be sought before proceeding. Stand-alone computers, which are those most commonly found, can be seized by any police officer or person named on a warrant.

(b) It is appreciated, however, that in the majority of cases, there will be no prior warning to the finding of a computer upon premises being searched. The investigator will have to decide on the best course of action, bearing in mind the nature of the investigation.

9.5 Briefing

(a) It is essential that all personnel attending at the search scene be adequately briefed, not only in respect of the intelligence, information and logistics of the search and enquiry, but also in respect of the specific matter of computers.

(b) Personnel should be encouraged to safeguard computer based electronic evidence in the same way as any other material evidence. Briefings should make specific mention, where available, of any specialist support that exists and how it may be summoned. Strict warnings should be given to discourage tampering with equipment by untrained personnel.

(c) Consider using visual aides to demonstrate to searchers the range of hardware and media that may be encountered.

9.6 Search Equipment

9.6.1 The following suggested, but not exhaustive, list of equipment may be of value during planned searches:

- Tools such as screw drivers (flathead and crosshead), small pliers, wire cutters for removal of cable ties;
- Production Schedule;
- Labels and tape to mark and identify component parts of the system, including leads and sockets;
- Production labels (tie-on and adhesive);
- Evidence Bags (general and anti-static);
- Cable ties for securing cables;
- Flat pack assembly boxes - consider using original packaging if available;
- Coloured marker pens to code and identify removed items;
- Camera and / or video to photograph scene in situ and any on screen displays;
- Torch.

9.7 Records to be Kept

(a) A Computer Evidence Seizure Log should be completed in full at the search scene. This will allow for the recording of the following:

- Sketch map of scene;
- Details of all persons present where computers are located;
- Details of computers - make, model, serial number;
- Display details and connected peripherals;
- Remarks/comments/information offered by user(s) of computer(s);

- Actions taken at scene showing exact time;

(b) On completion of the seizure the Computer Evidence Seizure Log should have a Documentary Production Backing Sheet attached and should then be lodged as a production in the case.

(c) The Cybercrime Examination Form should contain details of articles seized and submitted for examination along with detailed nature of the enquiry and the intended use of the material recovered.

10. Indecent Images of Children

10.1 Only specifically designated computer equipment and laptops should be used for the viewing or display of paedophile images.

10.2 For instruction / guidance refer to the Indecent Images of Children on Digital Media SOP and IT Security SOP.

11. Management of Digital Images

11.1 The capturing and recording of evidential images of incidents, e.g. subjects, scenes or injuries and being able to share that information with investigators, prosecutors and others involved in the criminal justice system, is a critical component of police work. A national review of the process for the capture, storage and submission of digital image files created by police officers has recently been completed and the new Guidance on the capture, storage and submission of Digital Images highlights these image files are to be treated as productions.

11.2 The guidance provides a nationally consistent approach including:

- Management and audit of equipment;
- Management and audit of digital storage media, including SD cards, USB memory sticks, portable Hard Disk Drives (HDD) and CD/DVD's;
- Handling of images;
- Submission of images to Forensic Services.

Appendix ‘A’

List of Associated Reference Documents

Policy

- Crime Investigation Policy
- Records Management Policy
- Data Protection Policy
- Information Security Policy

Standard Operating Procedures

- Crime Investigation SOP
- Productions SOP
- Indecent Images of Children on Digital Media SOP
- Internet, Research and Investigations SOP
- Communications Data SOP
- IT Security SOP

Guidance

- ACPO Good Practice Guide for Computer-Based Electronic Evidence
- Guidance on the capture, storage and submission of Digital Images
- Guidance Seizure and Forensic Examinations of Mobile Phones
- Mobile Phone Toolkit
- Cybercrime First Responders Guide
- Digital Forensic Examination Generic Risk Assessment Form

Appendix ‘B’

Glossary of Common Digital Media Terms

Address
The term address is used in several ways:

- An Internet address or IP address is a unique computer (host) location on the Internet.
- A Web page address is expressed as the defining directory path to the file on a particular server.
- A Web page address is also called a Uniform Resource Locator, or URL.
- An e-mail address is the location of an e-mail user (expressed by the user’s e-mail name followed by an "at" sign (@) followed by the user’s server domain name.

Archive File
A file that contains other files (usually compressed files). It is used to store files that are not used often or files that may be downloaded from a file library by Internet users.

Backup
A copy taken of all information held on a computer in case something goes wrong with the original copy.

BIOS
Basic Input Output System. A programme stored on the motherboard that controls interaction between the various components of the computer.

Boot
To start a computer, more frequently used as "re-boot".

Boot Disk
Refers to a floppy disk that contains the files needed to start an operating system.

Buffer
An area of memory, often referred to as a "cache", used to speed up access to devices. It is used for temporary storage of the data read from or waiting to be sent to a device such as a hard disk, CD-ROM, printer or tape drive.

Bulletin Board Service (BBS)
A BBS is like an electronic corkboard. It is a computer system equipped for network access that serves as an information and message-passing centre for remote users. BBSs are generally focused on special interests, such as science fiction, movies, Windows software, or Macintosh systems. Some are free, some are fee-based access, and some are a combination.

Byte
In most computer systems, a byte is a unit of data generally consisting of 8 bits. A byte can represent a single character, such as a letter, a digit, or a punctuation mark.

Cache
A cache (pronounced CASH) is a place to store something more or less temporarily. Web pages you browse are stored in your browser's cache directory on your hard disk. When you return to a page you've recently browsed to, the browser can get it from the cache rather than the original server, saving you time and the network the burden of some additional traffic. Two common types of cache are cache memory and a disk cache.

CDF
Channel Data Format, a system used to prepare information for Web casting.

CD-R
Compact disk – recordable. A disk to which data can be written but not erased.

CD-ROM
(Compact disk read-only memory or media) In computers, CD-ROM technology is a format and system for recording, storing, and retrieving electronic information on a compact disk that is read using laser optics rather than magnetic means.

CD-RW
Compact disk – rewritable. A disk to which data can be written and erased.

CMOS - Complementary Metal-Oxide Semi-Conductant
This is a low power version of a chip. It commonly holds the BIOS preference of the computer through power off with the aid of a battery.

CPU (Central Processing Unit)
The most powerful chip in the computer. Located inside a computer, it is the "brain" that performs all arithmetic, logic and control functions.

Cracker
A computer expert that uses his or her skill to break into computer systems with malicious intent or motives (cracking). The term was coined by Hackers to differentiate themselves from those who do damage to systems or steal information.

CRC (Cyclic Redundancy Check)
A common technique for detecting data transmission errors.

Cryptography
The process of securing private information that is sent through public networks by encrypting it in a way that makes it unreadable to anyone except the person or persons holding the mathematical key/knowledge to decrypt the information.

Database
Structured collection of data that can be accessed in many ways. Common database programs are: Dbase, Paradox and Access. Uses: various including – address links, invoicing information, etc.

Deleted Files

If a subject knows there are incriminating files on the computer, he or she may delete them in an effort to eliminate evidence.
Many computer users think that this actually eliminates the information. However, depending on how the files are deleted, in many instances a forensic examiner is able to recover all or part of the original data.

Denial of Service Attacks (DOS)
Denial of Service Attacks is aimed at specific Web sites. The attacker floods the Web server with messages endlessly repeated. This ties up the system and denies access to legitimate users.

Digital Signature
A code which is used to guarantee that an e-mail was sent by a particular sender.

Disk Cache
A portion of memory set aside for temporarily holding information read from a disk.

Disk Space
Disk storage. The space on the web hosting a company's server/computers that a website's content is allowed to utilise.

Dongle
A term for external hardware devices with some memory inside it. Companies that sell expensive software packages use dongles as proof that a computer actually has a licence for the software being used.

DVD
Digital versatile disk. Similar in appearance to a compact disk, but can store larger amounts of data.

Encryption
The process of scrambling, or encoding, information in an effort to guarantee that only the intended recipient can read the information.

E-Mail Header
E-mails come in two parts – the body and the header. Normal header information gives the recipient details of time, date, sender and subject. All e-mails also come with extended headers – information that is added by e-mail programs and transmitting devices – which shows more information about the sender that is in many circumstances traceable to an individual computer on the Internet.

Free Space
Can contain file clusters that are not currently used by the operating system but nevertheless contain deleted data.

Floppy Disk
These are disks that hold information magnetically. They come in 2 main types 3-inch and 5-inch. The 5-inch disks are flexible and easily damaged; the 3-inch disks are in a stiff case. Both are square and flat. Older machines may use larger or smaller sizes of disk.

Gigabyte (Gb)
1 Gigabyte = 1024 Megabytes. A gigabyte is a measure of memory capacity and is roughly one thousand megabytes or a billion bytes. It is pronounced Gig-a-bite with hard Gs.

Hacker
Persons who are experts with computer systems and software and enjoy pushing the limits of software or hardware. To the public and the media, they can be good or bad. Some hackers come up with good ideas this way and share their ideas with others to make computing more efficient. However, some hackers intentionally access personal information about other people with their expertise, and use it to commit computer crimes. See page 17, 'Cracker'.

Hard Disk
The hard disk is usually inside the PC. It stores information in the same way as floppy disks but can hold far more of it.

Hardware
The physical parts of a computer. If it can be picked up it is hardware as opposed to software.

Host Machine
For the purpose of this document a host machine is one which is used to accept a target hard drive for the purpose of forensically processing.

Imaging
Imaging is the process used to obtain all of the data present on a storage media (e.g. hard disk) whether it is active data or data in free space, in such a way as to allow it to be examined as if it were the original data.

Internet Relay Chat
A virtual meeting place where people from all over the world can meet and talk about a diversity of human interests, ideas, and issues. Participants are able to take part in group discussions on one of the many thousands of IRC channels, or just talk in private to family or friends, wherever they are in the world.

ISP – Internet Service Provider
A company that sells access to the Internet via telephone or cable line to your home or office. This will normally be free - where the user pays for the telephone charge of a local call - or by subscription - where a set monthly fee is paid and the calls are either free or at a minimal cost.

JAZ
A high capacity removable hard disk system.

Kilobyte (KB)
100.1 1 Kilobyte = 1024 bytes.

LINUX
An operating system popular with enthusiasts and used by some businesses.

Macro Virus
A virus attached to instructions (called macros) which are executed automatically when a document is opened.

Magnetic Media
A disk, tape, cartridge, diskette, or cassette that is used to store data magnetically.

MD5 HASH
An algorithm created in 1991 by Professor Ronald Rivest that is used to create digital signatures (i.e. fingerprints) of storage media such as a computer hard drive.

When this algorithm is applied to a hard drive then it creates a unique value. Changing the data on the disk in any way will change the MD5 value.

Megabyte (MB) 1 Megabyte = 1024 Kilobytes.

Memory
Often used as a shorter synonym for random access memory (RAM). Memory is the electronic holding place for instructions and data that a computer's microprocessor can reach quickly. RAM is located on one or more microchips installed in a computer.

Modem
Modulator/Demodulator. A device that connects a computer to a data transmission line (typically a telephone line). Most people use modems that transfer data at speeds ranging from 1200 bits per second (bps) to 56 Kbps. There are also modems providing higher speeds and supporting other media. These are used for special purposes – for example to connect a large local network to its network provider over a leased line.

Monitor
A device on which the PC displays information.

Mouse
Device that, when moved, relays speed and direction to the computer, usually moving a desktop pointer on the screen.

MS-DOS Microsoft – Disk Operating System
Operating system marketed by Microsoft. This is the most common operating system in use on desktop PCs, which automatically loads into the computer memory in the act of switching the computer on.

Operating System
This software is usually loaded into the computer memory upon switching the machine on and is a prerequisite for the operation of any other software.

ORB
A high capacity removable hard disk system. ORB drives use magneto resistive (MR) read/ write head technology.

Password
A word, phrase, or combination of keystrokes used as a security measure to limit access to computers or software.

PCMCIA Cards
Similar in size to credit cards, but thicker. These cards are inserted into slots in a Laptop or Palmtop computer and provide many functions not normally available to the machine (modems, adapters, hard disks, etc.).

Personal Computer (PC)
A term commonly used to describe IBM & compatible computers. The term can describe any computer useable by one person at a time.

Personal Organiser or Personal Digital Assistant (PDA)
These are pocket-sized machines usually holding phone and address lists, and diaries. They often also contain other information.

Pirate Software
Software that has been illegally copied.

Port
The word port has 3 meanings:

- Where information goes into or out of a computer, e.g. the serial port on a personal computer is where a modem would be connected;
- On the Internet Port often refers to a number that is part of an URL appearing after a colon (:) right after the domain name;
- It also refers to translating a piece of software to bring it from one type of computer system to another, e.g. to translate a window programme so that it will run on a Macintosh.

Public Domain Software
Programs that are 'free'.

Query
To search or ask. In particular to request information in a search engine, index directory, or database.

RAM
Random access memory is the PC's short-term memory. It provides working space for the PC to work with data. Information stored in the RAM is lost when the PC is turned off.

Removable Media

Items e.g. floppy disks, CDs, DVDs, cartridges, tapes that store data and can be easily removed.

Removable Media Cards
Small-sized data storage media which are more commonly found in other digital devices such as cameras, PDAs (Personal Digital Assistants) and music players. They can also be used for the storage of normal data files, which can be accessed and written to by computers. There are a number of these including:

- Smartmedia Card SD Expansion Card;
- Ultra-Compact Flash Compact Flash;
- Multimedia Card Memory Stick.

The cards are non-volatile – they retain their data when power to their device is stopped – and they can be exchanged between devices.

Shareware
Software that is distributed free on a trial basis with the understanding that if it is used beyond the trial period, the user will pay. Some shareware versions are programmed with a built-in expiration date.

Slack Space
The unused space in a disk cluster. The DOS and Windows file systems use fixed-size clusters. Even if the actual data being stored requires less storage than the cluster size, an entire cluster is reserved for the file. The unused space is called the slack space.

Smartcard
Plastic cards, typically with an electronic chip embedded, that contain electronic value tokens. Such value is disposable at both physical retail outlets and on-line shopping locations.

Software
The pre-written programs designed to assist in the performance of a specific task, such as network management, web development, file management, word processing, accounting or inventory management.

System Unit
Usually the largest part of a PC, the system unit is a box that contains the major components. It has the drives at the front and the ports for connecting the keyboard, mouse, printer and other devices at the back.

Tape
A long strip of magnetic coated plastic. Usually held in cartridges (looking similar to video, audio or camcorder tapes), but can also be held on spools (like reel to reel audio tape). Used to record computer data, usually a backup of the information on the computer.

Trojan Horse

A computer program, usually a virus that is hidden or disguised as another program or an e-mail. The victim downloads or starts what he or she thinks is a safe program and instead finds something actually designed to do harm to the system on which it runs.

UNIX
A very popular operating system. Used mainly on larger, multi-user systems.

USB Storage Devices
Small storage devices accessed using a computer's USB ports, that allow the storage of large volumes of data files and which can be easily removed, transported – and concealed. They are about the size of a car key or highlighter pen, and can even be worn around the neck on a lanyard.

Video Backer
A program, that allows computer data to be backed up to standard video. When viewed the data is presented as a series of dots and dashes.

Virus
A piece of programming code, which is inserted into other programming for the purpose of causing some unexpected and, for the victim, usually undesirable event. Viruses can be transmitted by downloading programming from other sites or be present on a diskette. Some are harmless (messages on the screen, etc.), others are destructive (corruption of information), while some may be fatal.

Windows
Operating system marketed by Microsoft. In use on desktop PCs the system automatically loads into the computer's memory in the act of switching the computer on. MS-DOS, Windows, Windows 3.0, Windows 95, Windows 98, .NET, Office XP, Windows XP and Windows Server are registered trademarks of Microsoft Corporation.

Windows NT
Operating system marketed by Microsoft primarily aimed at the business market. Multiple layers of security are available with this system.

Word Processor
Used for typing letters, reports and documents. Common Word Processing programs: Wordstar, Wordperfect, MS-Word.

Worm
Like a virus but is capable of moving from computer to computer over a network without being carried by another program.

Wireless Network Card
An expansion card present in a computer that allows cordless connection between that computer and other devices on a computer network. This replaces the traditional network cables. The card communicates by radio signals to other devices present on the network

Zip Drive/Disk

A 3.5-inch removable disk drive. The drive is bundled with software that can catalogue disks and lock files for security.

ZIP
A popular data compression format. Files that have been compressed with the ZIP format are called ZIP files and usually end with a .ZIP extension.