LIVE&BREATHE

Information Security Policy

Statement of Policy

It is the policy of the Live & Breathe to ensure that:

• Information will be protected against unauthorised access

• Confidentiality of information will be assured

• Integrity of information will be maintained

• Regulatory and legislative requirements will be met

• Information Security Training will be provided

• All breaches of Information Security, actual or suspected, will be reported and investigated

• Standards will be produced to support the policy. These include virus controls and passwords

• Business requirements for the availability of information and information systems will be met

• The Chairman has direct responsibility for maintaining the policy and providing advice and guidance on its implementation

• All Managers are directly responsible for implementing the policy within their business areas, and for adherence by their staff

It is the responsibility of each employee to adhere to the Information Security Policy.

Signed:

Name: Kenny Cox

Date: 19th April 2017

Introduction to the Policy

To ensure business continuity, minimise business damage and maximise return on investments and business opportunities, and indeed to comply with many of our client contracts, it is important that our business information is secure against all threats, internal or external. This is the aim of our Information Security Policy.

Our Policy affects staff, clients, suppliers, contractors and even visitors.

Information does not mean just computer-stored data. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or electronically, or spoken in conversation whether face-to-face or via telephone. And information can include all types of data from photographs to digital artwork files, databases containing business or consumer information through to personnel files. Much of this data is absolutely essential to the day to day running of the business and our ability to meet on-going client deadlines; it must therefore, as a matter of priority, be properly protected and maintained.

It is the intention of Live & Breathe to preserve:

- **confidentiality** - ensuring that information is accessible only to authorised users
- **integrity** - safeguarding the accuracy and completeness of information and processing methods
- **availability** - ensuring that authorised users have access to information and associated assets when required

Information security means that we can rely on being able to use information when we need it. It also brings confidence that it has not been tampered with and that we have control over who can see and use it.

There is no single, easy solution to achieving information security. It is not just about buying more computer software.

Information security is achieved by implementing suitable controls on:

- policies
- procedures
- organisational structures
- physical controls
- software functions

Legal requirements

Some aspects of Information Security are governed by legislation eg

- The Data Protection Act (1998)
- Copyright, Designs and Patents Act (1988
- Computer Misuse Act (1990)

In addition many of our client contracts have specific data protection requirements and each account group head should familiarise themselves with these requirements and ensure they are fully complied with by their whole account team.

Acceptable use of data/ information

All use of computer systems will comply with the Acceptable Use Policy described in the Staff Handbook. Acceptable use is defined as use for the purposes of:

1. Normal business use to enable the research, creation and production of creative solutions to clients' briefs
2. Other business research
3. Personal training/ educational development
4. Administration and management of the agency's business
5. Reasonable use of computer facilities for personal correspondence, where not connected with any commercial activity, within the guidelines stipulated in the Staff Handbook.

It is our policy that all use of the facilities shall be lawful, honest and decent, and shall have regard to the rights and sensitivities of other people.

Responsibilities

Management responsibilities

It is the responsibility of Directors, team heads and managers to ensure the following, with respect to their staff:

a) All current and future staff should be instructed in their security responsibilities.
b) Staff using computer systems/media must be trained in their use.
c) Staff must not be able to gain unauthorised access to any of Live & Breathe systems or manual data which would compromise data integrity.
d) Managers should determine which individuals are given authority to access specific information systems. The level of access to specific systems should be on a job function need, irrespective of status.
e) Managers should implement procedures to minimise Live & Breathe's exposure to fraud, theft or disruption of its systems.
f) Current documentation must be maintained for all critical job functions to ensure continuity in the event of relevant staff being unavailable.
g) All staff should be aware of the confidentiality clauses in their contract of employment.
h) Managers must ensure that the Head of IT/ Telecoms is advised immediately about staff changes affecting computer access (e.g. job function changes, leaving department or organisation) so that passwords may be withdrawn or deleted as appropriate.
i) Managers must ensure that all sub-contractors undertaking work for Live & Breathe have signed confidentiality (non-disclosure) undertakings.
j) Managers should ensure that all staff have access to, and have read, Live & Breathe's Information Security Policy.

Staff responsibilities

a) Each employee is responsible for ensuring that no breaches of information security result from their actions.
b) Each employee is responsible for reporting any breach, or suspected breach of security to their line manager/ a company director.

Head of IT and Telecoms' responsibilities

a) The job description for the Head of IT and Telecoms will include specific reference to the security role and responsibility of the post.
c) The Head of IT will be responsible to the Chairman for continued system security.
e) The Head of IT must ensure that only those persons who are authorised to have access are provided with that capability.

Proper use of communications

To ensure that Live & Breathe uses electronic, postal and verbal communications appropriately we will:

a) Ensure that staff are aware of the importance of checking the credentials of all callers requesting personal or other sensitive information.
b) Instruct staff and ensure that personal email addresses/ telephone numbers are not given to unknown callers.
c) Ensure that email is used according to the conditions described here and in the Staff Handbook. The use of email may be monitored.
d) Ensure that staff are aware of, and abide by the Acceptable Use Policy and are aware that use of the Internet may be monitored.
e) Ensure that fax communications are protected at all times and that faxes containing personal or sensitive information are sent and received in a secure manner.
f) Ensure that all staff are advised and regularly reminded of their obligation to respect the privacy of staff and third parties when using verbal communications. This means holding conversations discreetly and with due regard to the sensitivity of the subject under discussion.

Risk management

Good information security must be based on an understanding of the risks that we as a business actually face. The process of determining what those risks are and deciding what to do about them is our risk management process.

The risks

To manage risks we first need to identify threats to our business, as listed below:

- fraud, including identity theft
- burglary
- fire, flood and other natural disasters
- industrial espionage
- malicious damage
- computer viruses
- data loss
- loss of service

Vulnerability/ risk reduction

An assessment of these risks will be made for each information system to ensure that it is secured appropriately and cost effectively. Information systems within the agency face many risks which a Security Policy can reduce or eradicate.

Awareness

Managers are responsible for ensuring that all staff are aware of, and adhere to, this Information Security Policy. Departmental managers are responsible for ensuring their staff attend these awareness sessions. The Head of IT will ensure that Security is included in all Computer User Training.

Confidentiality agreements

Live & Breathe will continue to adopt comprehensive policies and procedures to ensure the secure handling of personal information within all information environments and complying with the Data Protection Act 1998.

All staff must sign an appropriate confidentiality (non-disclosure) undertaking contained in their Service Contract.

Business continuity

Objective

To be able to restore computer facilities to maintain essential business activities following a major failure or disaster.

Need for effective plans

Live & Breathe recognises that some form of disaster may occur, despite precautions, and therefore seeks to contain the impact of such an event on its core business through tested disaster recovery plans. We also recognise that IT systems are increasingly critical to our business and the protracted loss of key systems/user areas could be highly damaging in operational terms. We require tried and tested disaster recovery plans for our computing facilities to be maintained.

Planning process

The main elements of this process will include:-

- identification of critical computer systems
- identification and prioritisation of key users/user areas
- identification of likely disasters and what levels of disaster recovery are required
- identification of areas of greatest vulnerability based on risk assessment
- mitigation of risks by developing resilience
- developing, documenting and testing disaster recovery plans identifying tasks, agreeing responsibilities and defining priorities

Planning framework

Disaster recovery plans will cater for different levels of incident including:-

- loss of one office
- loss of a key operational area such as critical data/ media
- loss of a key part of a computer network
- loss of a computer's processing power
- loss of key staff

Disaster recovery plans will always include:-

- emergency procedures covering immediate actions to be taken in response to an incident and fallback procedures describing the actions to be taken to provide contingency cover defined in the disaster recovery plan
- resumption procedures describing the actions to be taken to return to full normal service
- testing procedures describing how the disaster recovery plan will be tested
- evidence of regular and adequate testing of plans

Equipment and software registers

Objectives

To identify the location and authorised use of Live & Breathe's computer assets

Equipment Inventory

An inventory of all computer and equipment and software will be maintained by the Head of IT. No one other than the Head of IT is authorised to purchase hardware.

Software Register
An up to date register of all proprietary software will be maintained to ensure that Live & Breathe is aware of its assets and that licence conditions are followed. This register will be maintained by the Head of IT. No one other than the Head of It is authorised to purchase software.

Access control to secure areas
Objective
To minimise the threat to Live & Breathe's computer systems through damage or interference.

Physical security
All central processors/ networked file servers/ central network equipment will be located in the IT room. Both our offices will be protected by intruder alarms and entrance to the offices will be via key/ intercom only. Both offices' alarm systems will be monitored by a guarding company.

The Leeds office will also be protected with bars/ grills at ground floor level and smoke cloaks at 1st floor level to protect the IT room. The Leeds IT room will be further protected with a keypad entry system to the room itself. Archived data disks/ hard drives will be stored in locked safes.

Security of third party access
Objective
To enable Live & Breathe to control external access to its systems.

Access control
No external agency will be given access to any of Live & Breathe's networks.

User access control
Objective
To control and limit individuals' access to systems to that required by their job function.

Access to Systems
Staff should only access systems for which they are authorised. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems for which staff have no authorisation. All contracts of employment have a non disclosure clause, which means that in the event of accidental unauthorised access to information, the member of staff is prevented from disclosing information which they had no right to obtain.

User password management
Passwords must be kept confidential. Passwords are the responsibility of individual users; they must not be used by anyone else even for a short period of time. The giving of a password to someone unauthorised, in order to gain access to an information system may be a disciplinary offence.

No staff should be given access to a live system unless properly trained and made aware of their security responsibilities.

Staff leaving Live & Breathe's employment
When a member of staff leaves the employment of Live & Breathe, their email account record is ended as part of the termination action carried out by the Head of IT.

Prior to an employee leaving, or to a change of duties, line managers will ensure that:

- passwords are removed or changed to deny access as appropriate

- the Head of IT is informed of the termination or change, and, where appropriate, the name is removed from authority and access lists
- passwords allocated to the individual should be removed and, if relevant, consideration given to changing higher level passwords
- reception staff and others responsible for controlling access to the office are informed of the termination, and are instructed only to admit in future as a visitor
- where appropriate, staff working out notice are assigned to non-sensitive tasks, or are appropriately monitored
- company/ departmental property is returned

The timing of the above requirements will depend upon the reason for the termination and the relationship with the employee. Where the termination is mutually amicable, the removal of data and systems access may be left to the last day of employment. Once an employee has left, it can be impossible to enforce security disciplines, even through legal process.

The Head of IT will delete or disable all identification codes and passwords relating to members of staff who leave our employment on their last working day. Prior to leaving, the employee's manager should ensure that all PC files of continuing interest to the business are transferred to another user before the member of staff leaves.

Managers must ensure that staff leaving Live & Breathe's employment do not inappropriately wipe or delete information from hard disks. If the circumstances of leaving make this likely then access rights should be restricted to avoid damage to information and equipment.

The Internet
Staff using computers and telephone equipment for Internet services must have their connection set up and approved by the Head of IT.

Housekeeping
Objective
To maintain the integrity and availability of computer assets.

Data Backup
Data should be held on a network directory where possible, to ensure routine backup processes capture the data. Such data must not be held on a PC or Mac hard drive.

Old data should be protected by clearly defined and controlled back-up procedures which will generate data for archiving and contingency recovery purposes. The backup copies should be clearly labeled and held in a secure area. Procedures should be in place to recover to a useable point after restart of this backup.

Archived and recovery data should be accorded the same security as live data and should be held separately preferably at an off-site location. Archived data is information which is no longer in current use, but may be required in the future.

Recovery data should be sufficient to provide an adequate level of service and recovery time in the event of an emergency and should be regularly tested to ensure that, in an emergency, the back-up data is sufficient and accurate. This can be done by automatically comparing it with the live data immediately after the back up is taken and by using the back-up data in regular tests of the contingency plan.

If live data is corrupted, any relevant software, hardware and communications facilities should be checked before using the back-up data. This aims to ensure that back-up data is not corrupted in addition to the live data.

Equipment, Media and Data Disposal
If a machine has ever been used to process personal data as defined under the Data Protection Act (1998) or "in confidence" data, then any storage media should be disposed of only after reliable precautions to destroy the data have been taken. Procedures for disposal should be documented.

Many software packages have routines built into them which write data to temporary files on the hard disk for their own purposes. Users are often unaware that this activity is taking place and may not realise that data which may be sensitive is being stored automatically on their hard disk.

Although the software usually (but not always) deletes these files after they have served their purpose, they could be restored and retrieved easily from the disk by using commonly available utility software. Therefore, disposal should only be arranged through the Head of IT who will arrange for disks to be wiped.

Software and information protection
Objective
To comply with the law on licensed products and minimise risk of computer viruses.

Licensed software
All users should ensure that they only use licensed copies of commercial software. It is a criminal offence to make/ use unauthorised copies of commercial software and offenders are liable to disciplinary action. Only the Head of IT is authorised to purchase and upload software and a database of software licences will be maintained.

The loading and use of unlicensed software on Live & Breathe computing equipment is NOT allowed. All staff must comply with the Copyright, Designs and Patents Act (1988). This states that it is illegal to copy and use software without the copyright owner's consent or the appropriate licence to prove the software was legally acquired. Live & Breathe monitors the installation and use of software by means of regular software audits; any breaches of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under the agency's Disciplinary Policy.

Unauthorised software.
We will only permit authorised software to be installed on our computer equipment.

Computers owned by Live & Breathe are only to be used for the work of Live & Breathe and for limited "essential" private use. The copying of leisure software on to computing equipment owned by Live & Breathe is not allowed. Copying of leisure software may result in disciplinary action under the Disciplinary Procedure. Computer leisure software is one of the main sources of software corruption and viruses which may lead to the destruction of complete systems and the data contained on them.

Virus control
Live & Breathe seeks to minimise the risks of computer viruses through education, good practice/ procedures and anti-virus software positioned in vulnerable areas.

Users should report any viruses detected/ suspected on their machines immediately to the Head of IT. No newly acquired disks from whatever source are to be loaded unless they have previously been virus checked by a locally installed virus checking package.

Users must be aware of the risk of viruses from email and the internet. If in doubt about any data received please contact the Head of IT for anti-virus advice.

Time-out procedures

Inactive terminals should be set to time out after a pre-set period of inactivity. The time-out facility should clear the screen.

Users should log off terminals or PCs/ Macs when leaving them unattended.

Equipment security

Objective
To protect IT equipment against loss or damage and avoid interruption to business activity.

Equipment siting and protection
IT equipment must always be installed and sited in accordance with the manufacturer's specification. Equipment must always be installed by the Head of IT.

Power supplies
Both offices will have a UPS backup to the mains electricity supply.

Network Security
It is the responsibility of the Head of IT to ensure that access rights and control of traffic on all our networks are correctly maintained.

It is the responsibility of the Head of IT to ensure that data communications to remote networks and computing facilities do not compromise the security of our systems.

Portable & hand-held computing equipment
Equipment, data or software must not be taken off-site by staff without documented management authorisation. (Management may provide authorisation on a 'once only' basis as long as it is subject to regular review)

Portable computers must have appropriate access protection, for example passwords and encryption and must not be left unattended in public places. Computer equipment is vulnerable to theft, loss or unauthorised access. Always secure laptop and handheld equipment when leaving an office and do not leave equipment unattended. When travelling, do not leave equipment/ data disks etc in cars or take them into vulnerable areas.

To preserve the integrity of data, frequent transfers must be maintained between portable units and the main system. The portable unit must be maintained regularly and batteries recharged regularly. Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times on or off Live & Breathe's premises. The equipment should only be used by staff to whom it is issued. All of the policy statements regarding the use of software and games apply equally to users of portable equipment belonging to Live & Breathe.

Users of this equipment must pay particular attention to the protection of personnel data and commercially sensitive data. The use of a password to start work with the computer when it is switched on is mandatory and all sensitive files must be password protected if encrypting the data is not technically possible. New users will be given training by the Head of IT in how to apply these passwords and other basic training in the use of a portable computer.

Users of portable equipment away from our premises should check their car and home insurance policies for their level of cover in the event of equipment being stolen or damaged and take appropriate precautions to minimise risk of theft or damage. Staff who use portable computers belonging to Live & Breathe must use them solely for business purposes otherwise there may be a personal Tax/ National Insurance liability.

Incident management

Emergencies are categorised into three categories:
• Physical security failure

• External failure
• Systems security failure
All users must contact the Head of IT through their line manager if they are aware of, or suspect, a security breach. The Account Director/ Director with board responsibility for the client must hold a review of each incident and report to the client their findings. Security breaches must be notified to the relevant client as soon as possible and in the case of a serious breach it may be necessary to escalate the matter to senior staff.

Incident management is documented in our Business Continuity Plan.

Electronic Mail (Email) Policy

Policy

Live & Breathe will provide employees with access to a variety of information technology systems and electronic communication media including Email for the pursuance of company business. With this access comes the following responsibilities:

Email

Care in drafting Emails

Users are responsible for drafting all emails carefully, taking into account any form of discrimination, harassment, Live & Breathe representation, and defamation of Data Protection issues. All emails must bear the company 'sign-off' and legal disclaimers. The Head of IT will set up each users' email system and sign-off and this must not be changed in any way by the user.

Staff Emails are a form of corporate communication and therefore should be drafted with the same care as letters. Before sending, proof read to make sure your message is understandable and appropriate. Do not send sensitive or emotional emails. Do not send emails in the heat of the moment. Never draft an email solely using CAPITALS – use normal sentence case. Users should be careful when replying to emails previously sent to a group.

Viruses and Attachments

The Head of IT will ensure that all incoming emails are scanned for viruses but staff have a responsibility to report suspicious emails to the Head of IT for inspection prior to opening any attachment.

Information Confidentiality

Email is an insecure method of communication with content easily copied, forwarded or archived. Sensitive data should not be sent by this means.

Intent to enforce and monitor

Live & Breathe reserves the right to carry out monitoring exercises on its systems, possibly without prior notice. Monitoring, via email blocking software may be used to block and read any email on the network at any time by the Head of IT.

Retention and Purging

Deletion of old emails must be managed by each individual user keeping in mind storage levels, archival levels, contractual evidence and legal discovery issues.

Personal use

These communication tools have been installed first and foremost to allow the business to function effectively in the 21st century. Our policy regarding private use of email and the internet is a 'reasonable use' approach. If staff wish to use the internet for private use they may do so outside of office hours or during lunch breaks and provided the duties outlined here are complied with.

Work email addresses should not be used for personal matters eg to place personal orders, sell private goods and services or make complaints. Such matters are unrelated to a member of staff's employment and using a work email can give the impression that the staff member is acting for, or on behalf of, Live & Breathe.

Email best practice

Junk mail
Email should not be sent to large numbers of people unless you are sure that it is directly relevant to their job. Sending unsolicited mail to many users ('spamming') is wasteful of user time and can disrupt the service, via performance delays, for other users.

Very large files
Sending of large files should be avoided where possible. The use of appropriately licensed compression software (e.g. zip files) is advised. Extremely large files should be sent by means other than email.

Protection of your terminal
Where terminals are left open and logged in when you leave your desk, a malicious user could send messages in your name. Ensure your terminal is locked, timed out or logged out.

Staff, Financial, Research, Client and Corporate Record Storage & Transportation
Objective
To identify and counter possible threats to Live & Breathe data and determine protocols for their storage and transportation.

Storage

Offices
All Staff, Financial, Research, Client and Corporate Records should be stored in a secure area (physical or electronic) and not left in an unattended, unlocked room or in an freely accessible part of the network. They should only be retained for the minimum length of time that they are absolutely required.

Elsewhere
All other areas where Records are stored should follow the best practice guidelines of being:
• Stored in a secure area
• Not left unattended
• Not kept for longer than necessary

Transportation
Where it is necessary to transport data outside the office, the individual is responsible for ensuring their security. Records should not be left unattended at any time. When being transported by car records should be stored in a concealed area. When using couriers ensure that a POD is obtained so you have evidence of delivery; if using Royal Mail, only send data by recorded post – do not use normal, non-recorded post.

Responsibility
All Staff who use, or come into contact with, confidential records are individually responsible for their safekeeping. Staff should be aware of their contractual and legal confidentiality obligations.

Homeworking Information Security Standards

Objective
To provide staff with information about the standards that should be used when they are working at home using computers (privately or company owned) and data.

This can be a confusing area and it is necessary to ensure that staff are informed and confident that they are doing the right thing. Today's technology allows a number of options about the way we work. We will continually study these options and develop appropriate protocols.

Use of person-identifiable data at home
Person-identifiable data files cannot be taken off site.

Transfer of personal data files
Person-identifiable data files must not be sent via email to a user's home mail box. The Information (Data Protection) Commissioner has advised that internet mail is not secure and should not be used to transmit confidential information.

Protecting data files
All electronic files used at home *must* be protected at least by file level password control.

Use of privately owned computers at home
All home PCs which are used for the manipulation of Live & Breathe data must have a current virus checker

System Configuration
All devices have been configured for specific use within the Live and Breathe environment. Any changes to the configuratiojn of the device can only be authorized by the Head of IT. This includes changing or removing password information.

Transportation of data or confidential documents
Staff must take reasonable care to minimise that risk of theft or damage. IT equipment must be transported in a clean, secure environment. During transfer of equipment between home and work equipment should be kept out of sight and not left unattended at any time. Computer equipment or manual data must not be left in cars overnight.

Storage of equipment
Staff must take all reasonable steps to minimise the visibility of computer equipment from outside the home, and to secure windows and doors when the home is unoccupied.

Storage of confidential data or reports
Staff must secure confidential data or reports that are not actively being used in the most secure area of their home.

<u>Legal requirements</u>
Data Protection Act (UK) 1998
The purpose of the Act is to protect the rights of the individual about whom data is obtained, stored and processed. The Act applies to both computerised and paper records.

Live & Breathe will comply with the registration requirements of the Data Protection Act 1998 and any replacement European Union (EU) law. This Act requires that appropriate security measures will be taken against unauthorised access to, or alteration, disclosure or destruction of personal data and against accidental loss or destruction of personal data.

The Act is based on eight principles stating that data must be:
• Fairly and lawfully processed
• Processed for limited purposes
• Adequate, relevant and not excessive

• Accurate
• Not kept longer than necessary
• Processed in accordance with the data subjects rights
• Secure
• Not transferred to other countries without adequate protection

Copyright, Designs and Patents Act 1988
This Act states that it is illegal to copy and use software without the copyright owner's consent or the appropriate licence to prove the software was legally acquired. The Head of IT is responsible for purchasing all items of software. All software purchased will have an appropriate licence agreement which may or may not be a site-wide licence.

The Head of IT will carry out periodic spot checks to ensure compliance with Copyright Law. Any infringement or breach of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under the Disciplinary Policy.

Computer Misuse Act 1990
This Act states that it is a criminal offence to attempt to gain access to computer information for which you have no authorisation. If it is suspected that any unauthorised access is made to a computer system then disciplinary action may be taken under the Disciplinary Policy.
On ending their employment employees must not disclose information which was confidential.

Antivirus guidelines
1. What is a Virus?
A computer virus is a damaging piece of software that can be transferred between programs or between computers without the knowledge of the user. When the virus software is activated (by incorporated instructions, e.g. on a particular date), it performs a range of actions such as displaying a message, corrupting software, files and data to make them unusable, and deleting files and/or data. While many of the viruses produced are benign and cause no real damage to the infected system, they always constitute a breach of security.

There are currently something like 60-75,000 known viruses and worms1 - some 10-20 new viruses or variants appear a day. When a virus or worm is released into the public domain, network worms and mass mailer viruses can sometimes spread worldwide before anti-virus vendors have had time to produce updates.

Even daily anti-virus updates are not always enough to ensure safety from all possible threats.

2. What do we do to prevent the spread of viruses?
Whilst precautions are taken at the network level to minimise the spread and impact of worms and viruses, it is not possible to make the process totally effective. Protection from viruses and worms is not a process that can be left entirely to system administrators and anti-virus software. The best efforts of administrators and security experts are not sufficient - all computer users must also play their part by taking simple precautions like those described below.

Avoid unauthorised software
Programs like games, joke programs, cute screensavers, unauthorised utility programs and so on can sometimes be the source of difficulties even if they are genuinely non-malicious. That is why it is forbidden for staff to install them. If such programs are claimed to be some form of antivirus or anti-Trojan utility, there is a high risk that they are actually in some way malicious.

Treat all attachments with caution
It makes sense to be cautious about email attachments from people you don't know. However, if attachments are sent to you by someone you do know, don't assume they must be OK because you trust the sender. Worms generally spread by sending themselves without the

knowledge of the person from whose account they spread. If you do not know the sender and / or are not expecting any messages from the sender about that topic, it is worth checking with the sender that they intended to send a message, and if so, whether they intended to include any attachment. If you were expecting an attachment from them, this may not apply. However, one recent virus sends out an email telling you that a "safe" attachment is on the way, then sends out mail with a copy of itself as an attachment.

Bear in mind that even legitimate, expected attachments can be virus infected: worms and viruses are related, but cause slightly different problems.

Regard anything that meets the following criteria with particular suspicion:

- If emails come from someone you don't know, who has no legitimate reason to send them to you.
- If an attachment arrives with an empty message.
- If there is some text in the message, but it doesn't mention the attachment.
- If there is a message, but it doesn't seem to make sense.
- If there is a message, but it seems uncharacteristic of the sender (either in its content or in the way it's expressed).
- If it concerns unusual material like pornographic web-sites, erotic pictures and so on.
- If the message doesn't include any personal references at all, (for instance a short message that just says something like "You must take a look at this", or "I'm sending you this because I need your advice" or "I love you!").
- If the attachment has a filename extension that indicates a program file such as those listed below.
- If it has a filename with a "double extension", like FILENAME.JPG.vbs or FILENAME.TXT.scr. As far as Windows is concerned, it's the last part of the file name that counts, so check that against the list below to find out whether it's a program like those listed, masquerading as a data file, such as a text file or JPEG (graphics) file.

In all the above instances, it is recommended that you check with the sender that they knowingly sent the mail/attachment in question or if this is not possible ask the Head of IT to check the file before opening it yourself.

Avoid unnecessary macros

If Word or Excel warn you that a document you're in the process of opening contains macros, regard the document with particular suspicion unless you are expecting the document and you know that it's supposed to contain macros. Even then, don't enable macros if you don't need to. It may be worth checking with the person who sent it to you that it is supposed to contain macros.

Be cautious with encrypted files

If you receive an encrypted (passworded) attachment, it will normally be legitimate mail from someone you know, sent intentionally (though the sender is unlikely to know in the event that they have a virus). However, that doesn't necessarily mean that it isn't virus-infected. If it started out infected, encryption won't fix it. Furthermore, encrypted attachments can't usually be scanned for viruses in transit: the onus is on the recipient to be sure the decrypted file is checked before it's opened. This goes not only for heavyweight encryption packages, but also for files compressed and encrypted with PKZip or WinZip.

Suspicious filename extensions

The following is a list of filename extensions that indicate an executable program, or a data file that can contain executable programs in the form of macros. This list is by no means all-inclusive. There are probably a couple of hundred filename extensions that denote an executable program of some sort. Furthermore, there are filenames like .RTF that shouldn't include program content, but sometimes can, while Word documents (for instance) can in principle have any filename extension, or none. Furthermore, zipped (compressed) files with

the filename extension .ZIP can contain one or more of any kind of file.
.BAT .CHM .CMD .COM .DLL .DOC .DOT
.EXE .FON .HTA .JS .OVL .PIF .SCR
.SHB .SHS .VBS .VBA .WIZ .XLA .XLS

Report It!
If you think that you may have received a virus - ***Report It!***

1 A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

2 In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus.

3 In Microsoft Word and other programs, a macro is a saved sequence of commands or keyboard strokes that can be stored and then recalled with a single command or keyboard stroke. A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it.

4 An executable file is a file that contains a program. It is a particular kind of file that is capable of being executed or run as a program in the computer. In a Windows operating system, an executable file usually has a file name extension of .bat, .com, or .exe.