

Virus Protection Procedures

In order to prevent the introduction of virus contamination into the Organisation's computer systems the following must be observed:-

1. unauthorised software including public domain software, magazine cover disks/CDs or Internet/World Wide Web downloads must not be used.
2. all software must be virus checked using standard testing procedures and authorised by the IT department before being used.
3. Staff should not attempt to disable or bypass the installed anti virus software in any way.

Use of computer equipment

1. The Organisation does not permit the loading or use of unauthorised software on any computer equipment. Employees doing so put The Organisation in danger of being prosecuted as well as risk introducing viruses to the systems.
2. Nor is it permitted to use The Organisation's software on any personal equipment.
3. It is forbidden to gain unauthorised access, or attempt to gain unauthorised access, to any data held by The Organisation.
4. Staff are not permitted to take copies of any material/data belonging to The Organisation. Anyone found breaking the above rules will be subject to disciplinary action which may result in the termination of your employment.
5. Staff are not permitted to use any form of data storage devices on site (data storage devices can include but are not limited to USB memory sticks, writable CDs/DVDs and removable Hard Drives).
6. All users are provided with a unique log on, staff are reminded that passwords should remain confidential between the company and you. Passwords should be changed on a frequent basis.

Email & Internet Policy

The purpose of the Internet and Email policy is to provide a framework to ensure that there is continuity of procedures in the usage of Internet and email within The Organisation.

All employees are required to observe the following rules which are enforced

Computer Usage Policy for [Organisation Name]

by The Organisation's disciplinary procedures which could include summary dismissal.

All employees will be formally trained on the use of email and Internet facilities, as applicable.

Access to email facilities are provided for communications relating to The Organisation.

You may/You May not (delete as appropriate) use email facilities for limited personal communications.

Any access to the Internet is provided for The Organisations benefit.

You may/You may not (delete as appropriate) use the Internet for limited personal reasons only during your authorised breaks.

Where appropriate, duly authorised staff are encouraged to make use of the Internet as part of their official and professional activities.

Attention must be paid to ensuring that published information has relevance to normal professional activities before material is released in The Organisation's name. Where personal views are expressed a disclaimer stating that this is the case should be clearly added to all correspondence. Any Intellectual Property rights and copyrights must not be compromised when publishing on the Internet.

Employees may not use the Internet facilities to access any of the following types of Website: *(amend as required)*

- Personal email (such as Hotmail, Gmail etc.).
- Shopping.
- Auctions.
- Travel (except directly connected with employees travelling on behalf of The Organisation).
- Social Networking.
- Political Sites.
- Forums (except those to which The Organisation subscribes).
- Pornographic.
- Gambling.
- Any site promoting violence or racial, religious or social prejudice or persecution.
- Any site of a defamatory nature.
- Any site promoting or involved in illegal activities.

Similarly no emails should be sent that reference any of the above topics.

Email usage guidelines

The use of the email system is encouraged as its appropriate use facilitates efficiency. Used correctly it is of assistance to employees. Inappropriate use however causes many problems including distractions, time wasting and legal claims.

The email system is available for communication and matters directly concerned with the legitimate business of The Organisation. Employees using the email system should give particular attention to the following points:

- All emails must comply with company communication standards.
- Do not send any restricted information unless this is specifically required as a part of your job.
- Where it is necessary to send restricted information, ensure that the procedures stipulated for the transmission of that information are followed.
- Email messages and copies should only be sent to those for whom they are particularly relevant. Take care to correctly enter the name of the intended recipient.
- Flame mails (i.e. emails that are abusive) must not be sent. Hasty messages sent without proper consideration can cause upset, concern or misunderstanding.
- If an email is confidential the user must ensure that the necessary steps are taken to protect confidentiality. The company will be liable for infringing copyright or any defamatory information that is circulated either within the company or to external users of the system.
- Offers or contracts transmitted by email are as legally binding to the company as those sent on paper.
- Do not send any emails that could constitute bullying, harassment or other detriment.
- Do not send any emails that transmit copyright information and/or any software available to The Organisation.
- Emails distributing confidential information about other employees, The Organisation or it's customers or suppliers are forbidden
- Do not open any attachments in emails you receive unless they are expected as part of the established procedures and are clearly identified as such.

Computer Usage Policy for [Organisation Name]

- Should your computer malfunction after opening any attachment report this to the IT support department.
- Report any SPAM emails you receive to the IT support department.
- Do not initiate or forward any “Chain” emails.
- If any email you receive makes you feel uneasy, report it to your manager.

Signed: _____

Print Name: _____

Date: ____ / ____ / ____