the VOLUNTARY NETWORK

ICT Policy

Introduction

1. Hardware and Software

Inventory (Appendix 1 & 2)

Keeping an up to date inventory of equipment and software can help:

- fixing problems
- future purchases
- developing systems

The ICT Manager is responsible for ensuring the inventory list is maintained.

Office set-up

It is best to avoid re-arranging how equipment is plugged in (computers, power supplies, network cabling, modems etc.). Therefore, before touching any such items the ICT Consultant must be consulted.

Care of Hardware

Computers and peripherals- external

Turning off the workstations (PC's, Printers, etc.) is the responsibility of each user, and the last person to leave the office must check that all equipment is turned off. Any equipment which should be left switched on (Router, Fax, etc.) must be clearly labelled.

Each user is responsible for the cleaning of their PC and associated peripherals.

Hard Drive maintenance

To keep PC's running at top performance, the hard drive needs a regular 'Clean Up' and 'Defragmenting'. These facilities are available in Windows under Start Menu>Programs>Accessories>System Tools.

Backing-up data

All core documents/databases will be backed up on memory devices, this process is set to run each Wednesday evening**.** Staff will leave their computer on when they leave, it will shutdown automatically following the pre-programmed back-up routine. The memory devices will be kept in a separate location.

Archiving

Staff should regularly clear their hard drive of unneeded documents, ensuring optimum performance.

Food and Drink

Liquid spilt on computers can cause problems; food on keyboards can cause them to jam. It is therefore the responsibility of all staff to ensure that food and drink is kept away from equipment.

New Equipment

All purchases are recommended and approved by the General Manager.

New Software

Hardware capacity

Before buying software, it is important to ensure there is the capacity on the computer(s) in terms of hard disk space and processor power and speed. The ICT consultant should check this before making any purchase.

Compatibility

As with hardware capacity, new software needs to be checked for total compatibility with the current system before purchase. No software must be installed without permission from the General Manager.

Upgrading software

It is recommended that any software upgrades are only made after Version 2 of the software has been released, to avoid using software before the initial flaws have been ironed out. The IT Support contractor will be responsible for ensuring that that any major software updates, in particular 'Service Packs' and relevant 'Patches' are provided and loaded, at least every six months.

Installing software

Software can clog up a computer and reduce its speed. Software, including demos, are now given away freely, and much of it is likely to be useless for the purpose of the business.

Staff must seek the permission of the General Manager before installing any software.

New Hardware

Before buying hardware, it is important to ensure that it will meet both current and future needs. The General Manager should check this with our IT Consultant before purchasing.

2. Use of Network

Printers

Each PC has access to at least one printer, either attached to that computer or through the network. In the event of a printer failure an alternative printer can be used via the network.

Users must ensure the correct paper is loaded in the printer before printing.

3. User Support

User Guide

Many computer / network problems can be solved by rebooting, so if a computer 'freezes' (doesn't respond to input from the keyboard or mouse), try the following:

- Press Ctrl + Alt + Del at the same time.
- If this doesn't work 'Reset' the machine rather than turning it off and on again.

If this doesn't solve the problem, contact the ICT Manager (or the senior person in the office) and request assistance from IT Support.

If contact with IT Support is approved then [Kevin Law, Digital Data Solutions 08701163500]. If the problem cannot be resolved over the phone IT Support will attend the office.

Recording the problem (Appendix 3)

Usually the problem will either be:

- A computer problem (be it hardware or software): The problem should be explained to the General Manager. Once this is fixed (usually by external help), the way it was fixed should also be noted in the log.
- Staff not knowing how to use the computer: If the issue was to do with staff training, the area of training need should be noted and appropriate training arranged.

4. Security

Viruses

Viruses can cause serious damage to computers. If everyone adopts good habits, and basic precautions are taken, the systems are unlikely to be affected by viruses.

Viruses are small programmes that can read and delete data on your computer's hard disk, forge e-mail messages to others in your name, change the way programs work on your PC, or cause other harm. Viruses can be transmitted when data travels from one computer to another, mainly as executable files (those ending in .exe) most commonly via attachments to emails, but they can also lurk on websites. Getting rid of viruses can be time-consuming, expensive: prevention is certainly better then cure.

Anti-virus software

Anti-virus software is the common way to keep viruses at bay. This software is installed on each PC and is configured to scan floppy discs for viruses before use, check incoming emails / downloaded files from the Internet, and scan the hard drive of the PC periodically for viruses.

To remain effective the anti-virus software must be updated regularly (every day), and this is performed automatically via the Internet.

Safety measures

To prevent possible infection from viruses all people should adopt the following rules:

- Download documents, and programs, only from trustworthy sources on the Web.
- Treat email attachments with caution, and do not open them if there is in any doubt as to the contents.

Data

Restricting access to data

Using passwords to prevent others accessing the data on your computers can help protect the business; users should avoid disclosing passwords or other security details to anyone else. It is advisable to change your passwords every 8 weeks.

Data Protection

The Data Protection Act 1998 requires organisations to register the information they hold about people, and what they do with it. You are then legally bound to use it within these parameters. The 1998 Act that came into force in March 2000 is intended principally to protect people rights. It allows people more information about who is doing what with their data.

The General Manager is the Data Protection Compliance Officer and as such is responsible for Data Protection.

5. Internet Use

Internet

The Internet provides access to a valuable source of information. Regularly visited websites, that are relevant to the business, are listed in the 'favourites' folder.

Large quantities of data

Be aware of storing, transmitting or handling large quantities of data, particularly images or audio and video. These large files use up disc space very quickly and can bring a network to a standstill.

Email

Email can provide fast and cost-effective communication:

- Use it in preference to paper to reach people quickly (saving time on photocopying / distribution) and to help reduce paper use.
- Use the phone for urgent messages (email is a good backup in such instances).

Email Good Practice Tips:

Using it

Have your email program open and check your in-box regularly.

Filing it

Keep your in-box fairly empty so that it just contains items requiring your action. Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the email in a folder, or extract the useful information and save it somewhere logical). Keep electronic files of electronic correspondence, only keeping what you need to.

Avoid printing emails and keeping paper files.

Email address

Each person who uses email is encouraged to update any records in the address book with changes.

Checking

Think and check messages before sending (just as you would a letter).

Your opinion

When sending information externally, be aware that you could be seen as speaking on your businesses behalf. Make it clear when opinions are personal and be aware that other people might not share your sense of humour!

Attachments

Since viruses are most commonly sent via email, you must not open email attachments unless you have a good expectation of what it contains.

6. Personal use of Systems

Be considerate about storing personal files on PC's. Screen saver images require much more disc space and vary greatly and must not be downloaded from the Web.

Use of facilities for leisure or personal purposes (e.g. sending and receiving personal email, browsing the Internet) is permitted so long as such use does not:

- incur specific expenditure for the organisation
- impact on your performance of your job
- break the law
- bring the business into disrepute

7. Misuse of Systems

Licences

Software needs to be used legally in accordance with the relevant licensing and copyright agreements. Copies of all software licences and agreements are filed in the ICT Inventory.

Use

It is illegal to obtain unauthorised access to any computer or to modify its contents. Anyone who does not have access to information resources they feel they need should contact the General Manager.

A deliberate and serious breach of the policy will lead to disciplinary measures that may include the offender being denied access to computing facilities.

Electronic monitoring

Any information available within the ICT facilities will not be used to monitor the activity of individual staff in anyway without their prior knowledge, except:

- in the case of a specific allegation of misconduct, when mangers can authorise accessing of such information when investigating the allegation
- if such information cannot avoided whilst fixing a problem

In such instances, the person concerned will be informed immediately and information will not be disclosed wider than is absolutely necessary. In the former case, their access to ICT facilities may be disabled pending investigation.

Dated August 26, Review August 28