Policy 35 - IT Policy

CONTENTS

PROCEDURES FOR ALL IT USERS

1. First ensure you have permission from the appropriate person/s to use the equipment.
2. Ensure you log on before using the equipment. If unfamiliar with logon procedure ask a member of the IT section.
3. Ensure no food or drink is consumed while using the equipment. (Health & Safety).
4. If you are paying client, ensure you return to the receptionist the login form for payment of time/materials/internet use.
5. Ensure you leave the work are clean and tidy after use.
6. When printing ensure you know which printer to use, if not ask a member of the IT section.
7. If using your own floppy disk ensure it has been checked for viruses by a member of the IT section before use.
8. Do not install or delete any programmes without prior permission.
9. Remember to follow copyright law and the data protection act at all times when using the software or the Internet.
10. Last but not least, if in doubt ASK.

⊙⊙⊙⊙⊙⊙⊙⊙⊙

INTRODUCTION

Welcome to LD Training whilst we hope your course proves enjoyable, stimulating and successful, it is important that it is realised that you will be using computer hardware and software which can readily be used to produce and store information not necessarily just for your course. It is therefore essential that Local as well as Legal procedures and regulations are practiced in the operation of this equipment.

It is to give an over view of the responsibilities that apply to all users of equipment within the LD Training organisation that this hand out has been produced, so that we all benefit from smooth running systems, while the risk of damaged or lost files, data theft and virus contamination is minimised.

The good practice described here is similar and just as important when using computers outside of LD Training.

The regulations and procedures properly applied protect all individuals and are essential to the smooth running of the centre.

⊙⊙⊙⊙⊙⊙⊙⊙⊙

REGULATIONS AND PROCEDURES

Everyone who uses a computer or computer system in the centre, including Staff, Clients and Visitors must read this booklet and follow the regulations and good practices described. It is the responsibility of all Staff, Clients and Visitors to ensure that they are complying with LD Training practice by checking with the IT staff if they are unsure of any procedural use.

You have a personal responsibility:

- To take appropriate measures to protect computer equipment, systems and information.
- To protect access to computer systems and data files.
- To protect sensitive information
- To protect data about people.
- You may only use computer equipment for training or company use unless otherwise authorised by an appropriate member of staff.

You are not permitted:

- To misuse or attempt unauthorised access to any computer equipment.
- To use unlicensed or unauthorised software.

⊙⊙⊙⊙⊙⊙⊙⊙⊙

GENERAL

- If you suspect or become aware of a security problem report it to your supervisor or an appropriate member of staff immediately.
- No equipment, disks or training materials may be taken off the site.
- Do not bring or use disks from outside LD Training unless expressly authorised to do so.
- You are responsible for any equipment that you are using.

⊙⊙⊙⊙⊙⊙⊙⊙⊙

PASSWORDS (STAFF ONLY)

- Password protection may only be set with the express authority of the appropriate staff.
- LD Training will set passwords
- You are responsible for keeping your password secret.
- If you think your password is known, change it.
- Please anticipate our IT support to change passwords as needed and at regular intervals
- Make it harder to guess a password by using a combination of at least six letters or numbers, for example; DIG8IT.
- Avoid easily guessed passwords such as:
  - Dates, family names, nicknames or car registration.
  - Themes e.g. names of Cars.
  - Sequences such as REX01, REX02……

If you are absent for an extended period or are leaving then please ensure you pass all passwords to the IT Staff.

The DSP and team will liaise to ensure staff are aware of their training requirements and are notified in a timely manner when it is due for renewal.

⊙⊙⊙⊙⊙⊙⊙⊙⊙

BACK-UPS

Your work can be destroyed by a mistake, machine fault, computer virus etc. so in order to protect it from loss.

BACKUP YOUR FILES AT LEAST AT THE END OF EVERY SESSION.

Minimise risk of loss of work by taking regular back ups (saving or copying your files) during your work session. The more often you do it, the less time will be spent recovering or repeating work.

Ideally back up disks should be stored away from the machine, so that if the machine is destroyed the disk and data will not be.

⊙⊙⊙⊙⊙⊙⊙⊙⊙

SENSITIVE INFORMATION

You have a personal responsibility to protect sensitive information.

When handling sensitive information, including data about people:

- Don't refer to it without need or talk about it socially.
- Beware of people trying to obtain information to which they're not entitled, particularly over the phone.
- Use document passwords to restrict who can read files.
- Never leave a computer screen displaying information.
- Site computer screens so unauthorised people can't read them.
- Lock away back-up disks.
- Before disposing of disks and paper, destroy data by fully reformatting or shredding.
- All screens must be set to time out at 3 minutes of non-use. A password must be enabled to re-access the screen

One should always check with an appropriate member of staff if you're uncertain about what you may disclose or whether information should be classified as restricted or confidential.

⊙⊙⊙⊙⊙⊙⊙⊙⊙

DATA ABOUT PEOPLE

You have a personal responsibility to protect data about people.

Many countries, including the UK, have Data Protection legislation to protect privacy by regulating the use of facts or opinions about individuals, such as employees and customers, even "just" names or addresses.

YOU MUST NOT HOLD DATA ABOUT PEOPLE UNLESS APPROVED BY AN APPROPRIATE MEMBER OF STAFF, AND IF YOU DO, ALWAYS FOLLOW THESE DATA PROTECTION PRINCIPLES.

Data about people must be:

- Obtained and used fairly and lawfully.
- Held only for stated and lawful purposes.
- Used or disclosed only for those purposes.
- Adequate, relevant, and not excessive for those purposes.
- Kept no longer than is necessary for the stated purposes.
- Shown to the individual concerned at their requests, and corrected or erased where appropriate.
- Protected by appropriate security measures against unauthorised access, alteration, disclosure or destruction and against accidental loss or destruction.

⊙⊙⊙⊙⊙⊙⊙⊙⊙

USE OF COMPUTER EQUIPMENT

YOU MAY ONLY USE COMPUTER EQUIPMENT FOR ORGANISATIONAL BUSINESS, UNLESS AUTHORISED BY AN APPROPRIATE MEMBER OF STAFF.

There are no circumstances in which you may use the organisations computers for purposes that are unlawful, offensive, interfere with the organisations business or may bring the organisations reputation into disrepute.

⊙⊙⊙⊙⊙⊙⊙⊙⊙

COMPUTER MISUSE

YOU ARE NOT PERMITTED TO MISUSE OR ATTEMPT UNAUTHORISED ACCESS TO ANY COMPUTER EQUIPMENT OR SYSTEM.

Before using any of the equipment contained within the organisation one should get clear guidelines from a member of staff about:

Which computer equipment and systems you may use.
The extent to which you may see, change, remove and disclose the information involved.

If you are in any doubt about whether you have permission to access any computer equipment, system, or data contained within such, then one should check with a member of staff first.

IN THE UK IT IS A CRIMINAL OFFENCE TO CAUSE COMPUTER INFORMATION TO BE ALTERED OR REMOVED WITHOUT AUTHORISATION.

Don't access, interfere with, switch off, remove or disclose details of security software or codes, including virus protection software unless you are specifically authorised by an appropriate member of staff.

⊙⊙⊙⊙⊙⊙⊙⊙⊙

SOFTWARE LICENSES

YOU ARE NOT PERMITTED TO USE UNLICENSED OR UNAUTHORISED SOFTWARE.

Making an unauthorised copy of software is a form of theft and therefore illegal. Also remember that computer viruses and other malicious programs are often spread by using unauthorised software.

This applies to all kinds of programs, including for example "shareware", "public domain" and screen savers, from all sources such as the Internet, colleagues, friends, home, magazines, mail shots, schools, trading partners, or anywhere else.

In any computing environment one may only use software purchased through official channels.

To avoid breaking license conditions:

- **DON'T TAKE UNAUTHORISED COPIES OF SOFTWARE.**
- Ensure license arrangements are adequate for the number of users.
- After updating software remove old copies.
- Remove all software before disposing of computer equipment or media.

You must tell an appropriate member of staff if you think there's software on an organisations computer that isn't approved or properly licensed.

⊙⊙⊙⊙⊙⊙⊙⊙⊙⊙

COMPUTER VIRUSES

A computer virus is a program that can make copies of itself. It can spread whenever information is passed from one computer to another, for example through disks, including CD-ROM and computer networks. Viruses disrupt business, waste time and can corrupt or destroy data.

To minimise the chance of virus infection:

- One must not use any disks or software that have not been supplied or approved by LD Training.
- Never use or transfer software from a public network.
- Check all disks received for viruses.
- Regular virus checks should be made of all disks used.
- Remove a USB as soon as you've finished with it and check there isn't one in the computer before switching on