SECTION F

DATA PROTECTION LEGISLATION

Content

F.1. INTRODUCTION

This section is intended to be read by all users of computers, including personal computers, who store in any shape or form, personal information about other people in computer records.

Although primarily within the UK Data Protection Act, staff at overseas sites may find the principles similar to equivalent Acts within their own territory.

The following are referred to as "The Act" in this leaflet:

- ⇒ The UK Data Protection Act 1984
- ⇒ The Data Protection (Jersey) Law 1987
- ⇒ The Data Protection (Bailiwick of Guernsey) Law 1986
- ⇒ The Data Protection (Isle of Man) 1986
- ⇒ The Data Protection Act 1998

Computers are in use throughout society - collecting, storing, processing and distributing information. Much of that information is about people - "personal data" - and is now subject to Data Protection legislation.

The Act applies only to information that is processed by a computer and relates to living individuals. It does not cover information, which is held and processed manually, i.e. in ordinary paper files, nor does it cover information that relates only to a company or organisation. HOWEVER, it is expected that a new European directive will make at least some manual records subject to Data Protection law.

This information has been produced in compliance with the Act. Its purpose is to provide information of a general nature. If you require more detailed information or advice on any aspect of the Act you should refer direct to the Data Protection Registrar.

F.2. PURPOSE

The purpose of the Data Protection Act 1984 & 1998 is to protect information held about people on computers and to provide a framework of standards, which govern the processing of such information by law.

a) Under the Act employees are entitled to :-

b) access personal data about themselves held on computer,

c) have any inaccuracy erased or corrected,

d) in extreme cases, obtain compensation for any damage or distress caused because personal data has been lost, destroyed, or because it is inaccurate or has been disclosed for an unauthorised purpose.

The Company policy is to be quite open about the reasons why it is necessary to collect personal data and Managers should ensure that they and their staff who handle personal data are aware of the following :-

F.3. MANAGERS' RESPONSIBILITIES

1) To ensure that any personal data collected is relevant, adequate and held for no longer than necessary.

2) To ensure that personal data collected for one purpose is not disclosed to other persons or organisations for other purposes.

3) To ensure that personal data held by the Company is secure.

4) To ensure that individuals concerned have access to their personal data so that they may reassure themselves that the Company operates properly while protecting their confidentiality and interests.

F.4. DEFINITIONS

The Act uses the following words and phrases. It is important to grasp their meaning because they define how the Act works.

Personal Data	Any information recorded on a computer about living identifiable individuals.
Data User	People or organisations who control the content and use of personal data.
Data Subjects	Individual(s) (about whom data held) such as customer, staff member or supplier.
Holding Personal Data	Personal data is 'Held' if the information relates to living individual and is automatically processed by reference to that individual, e.g. by name or account number.
Registration	Data users are required to register with the Data Protection Registrar all the purposes for which they hold personal data.
Computer Bureaux	Those who process personal data on behalf of data users or who allow others to use equipment in their procession for the processing of personal data.

F.5. THE DATA PROTECTION PRINCIPLES

The Act give rights to individuals about whom information is recorded on computer. They may find out information about themselves, challenge it if appropriate and claim compensation in certain circumstances. The Act places obligations on those who record and use personal data (Data Users). They must be open about that use and follow sound and proper practices (the Data Protection Principles). The Data Protection Registrar oversees the operation of the Act.

To comply with the Act, staff must observe the eight Data Protection Principles contained in it. Much of their content is line with normal practices and procedures, yet there are aspects of the principles that require emphasising. The Section describes the eight principles, together with an interpretation for the guidance of staff.

FAILURE TO FOLLOW THE PROVISION OF THE ACT MAY RENDER MEMBERS OF STAFF PERSONALLY LIABLE TO PROSECUTION, PARTICULARLY IF THEY ARE ALSO FAILING TO OBSERVE THE INTERNAL PROCEDURES

FIRST PRINCIPLE

"THE INFORMATION TO BE CONTAINED IN PERSONAL DATA SHALL BE OBTAINED, AND PERSONAL DATA SHALL BE PROCESSED, FAIRLY AND LAWFULLY".

This principle is concerned with the method of collecting the data, and the data subjects reasonable expectations of the purpose for which the data may be used. The data subject should not be misled or deceived in the collection of the data.

Careful consideration of this principle is required whenever a new use of existing data is proposed, or new data is collected for a new or existing purpose, e.g. direct marketing.

SECOND PRINCIPLES

"PERSONAL DATA SHALL BE HELD ONLY FOR ONE OR MORE SPECIFIED AND LAWFUL PURPOSES".

Data users must be registered with the Data Protection Registration for each purpose for which they hold personal data.

Each registration may have several different purposes.

Each register entry indicates:

a) The purposes for which the personal data is held. Any such holding would be a criminal offence under the Act.

b) For each purpose listed, the data subjects and the types of personal data held.

c) Sources from which the personal data is obtained and persons or bodies to whom it is disclosed are listed. It is a criminal offence to obtain or disclose data outside those listed.

d) Transfers of data overseas are shown either by named country or as being world-wide.

THIRD PRINCIPLES

"PERSONAL DATA HELD FOR ANY PURPOSE OR PURPOSES SHALL NOT BE USED OR DISCLOSED IN ANY MANNER INCOMPATIBLE WITH THAT PURPOSE OR THOSE PURPOSES".

The Data User must use personal data only for the purpose(s) registered. This includes making only those disclosures that are registered.

Normal requirements for confidentiality also require that staff do not disclose data to other than a legitimate disclosee.

FOURTH PRINCIPLE

"PERSONAL DATA HELD FOR ANY PURPOSE OR PURPOSES SHALL BE ADEQUATE, RELEVANT, AND NOT EXCESSIVE IN RELATION TO THAT PURPOSE OR THOSE PURPOSES".

Consideration should be given as to why particular information is held. This should normally apply at the time the decision to hold the data is first taken.

FIFTH PRINCIPLE

"PERSONAL DATA SHOULD BE ACCURATE AND WHERE NECESSARY KEPT UP TO DATE".

It is normal practice to ensure accuracy of data. Staff must continue to follow any procedures set up to maintain and update data. Errors must always be corrected promptly.

A data subject may obtain compensation for any damage and distress suffered as a result of inaccurate data.

SIXTH PRINCIPLE

"PERSONAL DATA HELD FOR ANY PURPOSE OR PURPOSES SHALL NOT BE KEPT LONGER THAN IS NECESSARY FOR THAT PURPOSES OR THOSE PURPOSES".

Procedures must exist to ensure the deletion of data when it is no longer necessary for the purpose for which it is being held.

SEVENTH PRINCIPLE

"AN INDIVIDUAL SHALL BE ENTITLED -

a) AT REASONABLE INTERVALS AND WITHOUT UNDUE DELAY OR EXPENSE

i) TO BE INFORMED BY ANY DATA USER WHETHER HE HOLDS PERSONAL DATA OF WHICH THAT INDIVIDUAL IS THE SUBJECT, AND

ii) TO ACCESS TO ANY SUCH DATA HELD BY THE DATE USER, AND

b) WHERE APPROPRIATE, TO HAVE SUCH DATA CORRECTED OR ERASED".

All personal data, with very limited exceptions, must be made available to a data subject within 40 days of receipt of a valid request.

Care must be exercised that information is not recorded which would prejudice the holder if that information was disclosed to the data subject, eg expressions of opinion about a customer.

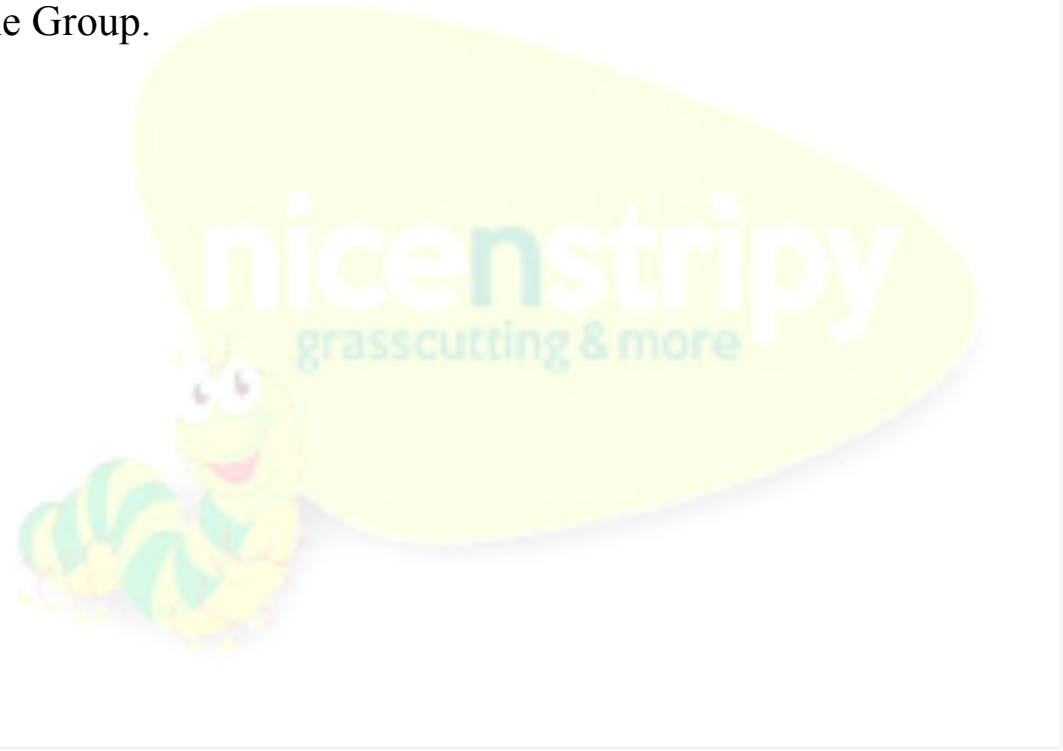
An individual has the right to correction or erasure of personal data only when such a request is considered 'appropriate', i.e. when necessary for ensuring compliance with the other Data Protection Principles, e.g. when the personal data is irrelevant or inaccurate.

Any offices, which receive a subject access request, must forward it to the relevant Data Protection Co-ordinator without delay.

EIGHT PRINCIPLE

"APPROPRIATE SECURITY MEASURES SHALL BE TAKEN AGAINST UNAUTHORISED ACCESS TO, OR ALTERATION, DISCLOSURE OR DESTRUCTION OF, PERSONAL DATA AND AGAINST ACCIDENTAL LOSS OR DESTRUCTION OF PERSONAL DATA".

Extreme care must be taken to prevent unauthorised access to any data, and proper backups must be taken regularly. No employee should take any action that could result in unauthorised disclosure or access to any personal data held by the Group.



F.6. GENERAL DATA PROTECTION ISSUES

F6.1. ALL-IN-1

ALL-IN-1 Users must be aware of the way in which the Data Protection Act affects the way in which information is created and stored.

Any document or message concerning an individual which is filed in an ALL-IN-1 folder, the name of which is such that documents or messages are able to be retrieves from folders, is liable to subject access.

Any names or keywords associated with personal data, which occur in the body of a document, should not be regarded as liable to subject access. This is intended to avoid the ludicrous situation that would otherwise obtain where every document containing a name would be subjected to the DP Act.

ALL-IN-1 can present problems for subject access as personal data could be held in folders by a number of users whose relationship with the requester is not obvious, eg information relating to job interviewees.

To keep subject access searches to a manageable number, wherever possible folder names and keywords should be kept to a minimum.

F6.2. TEST DATA

Personal data held for testing purposes must be subject to the same stringent security procedures as live data. A data subject is technically entitled to a copy of such data, although you would not send it unless specifically requested.

F6.3. TRANSBORDER DATA FLOW

Trans-border Data Flow (TDF) is that element of Data Protection legislation concerned with the movement of information across national boundaries.

As a general rule, countries that have a Data Protection Act (or an equivalent such as a Privacy Act) will permit the export of data, provided the target country also has a Data Protection Act offering similar levels of protection as its own.

Currently, the UK Data Protections Act only covers personal data. Certain other countries have wider reaching legislation which also covers non-personal data (such as companies, partnerships, institutions, "legal persons", etc) and, in some cases, manual records

NO PERSONAL DATA SHOULD BE TRANSMITTED ABROAD WITHOUT FIRST CHECKING THAT THE INFORMATION DOES NOT CONTRAVENE THE ACT.