UNIVERSITY OF EDINBURGH
Edinburgh Regional Computing Centre

User Note 99

(November 1986)

Title: **University of Edinburgh Code of Practice for the Security of Computer-Based Personal Data Files**

Author: Edinburgh University Data Protection Working Party

Contact: Advisory service

Software Support Category: n/a

Synopsis

The code of practice in this Note contains the University's official guidance on security measures to prevent personal data stored on a computer from being lost, disclosed or tampered with.

Keywords

Data Protection Act, personal data, security

For the purposes of this Code of Practice, and for the Data Protection Act generally, "personal data" is information about a living individual which is in a form in which it can be processed automatically. "Personal data" need not be sensitive or confidential; it is "personal" because it relates to a living individual.

University of Edinburgh
Code of Practice for the Security of Computer-Based Personal Data Files

1. Introduction

Preventing loss or disclosure of personal information held or printed from a computer to unauthorized sources is the responsibility of the owner or user of such personal information.

The suggested code of practice is not foolproof but it does provide a good level of security and if followed will result in an owner or user having taken reasonable precautions to secure the personal information he or she holds.

2. Passwords

No amount of system software can protect your data if it is easy for someone else to find out your password, because you have written it down or have made it easy to guess. Choose a password with at least 8 characters (not all the same) and use a different one for different machines, or for different processes on the same machine.

If you discover that someone else knows your password change it immediately. In any case you should change your password periodically - some systems can be programmed to remind you on, say, the first day of each month.

Remember to change your background (batch mode) password as well as your foreground (interactive mode) one, if the system has passwords for each mode. Security can be breached in batch mode and systems are often less rigorous in their precautions against this than they are in interactive mode.

3. Printed Output

This covers various forms of hard copy output, though output to printers will be the main form.

It may often be possible to arrange that output from a file containing personal data does not contain enough information to enable individuals to be identified. In that case no special precautions are needed.

If individuals can be identified (subject to the qualification below) the output should be routed to a device under your control, for example a private printer, in an area which is not accessible to people who are not entitled to see the output. The people who are entitled to see the output are fellow employees who need to see it in the course of their work, and other people who are named, explicitly or by description, as potential recipients in the registration of the original data.

There is an area of uncertainty with regard to information which is publicly available. In simple cases such information need not be protected, but collations of publicly available information may bring together facts which, when combined, are regarded as sensitive by the individuals concerned. In such cases the output should be sent to a device under your control.

Printed output from a computer should not be left lying around an office for anyone to see in passing or to browse through. Put it out of sight and in a secure place.

When disposing of computer printouts containing personal information do not throw them in the waste-paper-basket or leave them lying on a shelf to gather dust. Always have the printouts shredded or arrange for them to be disposed of as confidential waste.

4. Microcomputers

(a) Whenever finishing a session at the microcomputer or leaving the office for whatever reason never leave the microcomputer unattended or with someone else present who does not have the right of access to your information files. Make it a habit to:
- Remove diskettes from the microcomputer.
- Switch off your microcomputer.
- Put your diskettes away in secure accommodation such as a filing cabinet and lock it keeping the key on your person.
- If your microcomputer has a hard disc then make sure that whenever you leave your place of work that you have secured your microcomputer. This can be done by locking your office, or, if your work place is in an open or shared office, then password protection of the files should be used (see (b) below).
- Some of the new microcomputers such as IBM PC/AT can be locked and if your microcomputer is lockable then lock it as well.

(b) Whenever possible protect your information files with a password. Do not, however, leave yourself reminder notes of the passwords displayed around your working place.

(c) When you have no further use for an information file then you should erase it from the active diskette and also erase any backup copies you have.

(d) When you find a diskette contains information which is all obsolete then it should be cleared by using the Format procedure.

(e) Position the microcomputer and its display screen so that the information it displays is not seen by people who are not entitled to see that information. This is particularly relevant to microcomputers situated in an open or general office where some of the people passing through the office are not authorized users of the information.

5. Terminals

(a) Always log off at the end of a session or before leaving the terminal unattended. In the case of screen-based terminals, always clear the screen after logging off.

(b) In the case of hard-copy terminals, the practices outlined in Section 3 on Printed Output should be followed.

(c) Where the data to be displayed on a terminal contains enough information to enable individuals to be identified, then the terminal to be used should be located in an area which is only accessible to people who are entitled to see the output.

6. Data Files

(a) File Access Permissions
If the computer system is a multi-user one which allows files to be granted

differing access permissions for different user processes, then care should be taken to ensure that only authorized users are permitted access. In particular, the file access permission should not be set to allow global access enabling all users of the system potential access to it.

(b) Levels of Sensitivity

Clearly, deciding how sensitive a particular set of data is will be an essentially subjective process dependent on a variety of factors relating to the nature of the data and the data subjects. The data user is normally in the best position to judge the level of sensitivity of the data under his control. In reaching a decision, however, it may be useful to consider the following two questions in respect of unauthorized disclosure or loss of information:

(1) How upset would the data subject be?

(2) How much damage could be caused?

The answers to these questions will tend to place data into one of two classes:

(A) Where there might be some damage done by loss or disclosure, and the data subject might be annoyed or irritated - but no more than that;

(B) Where significant damage would be done by loss or disclosure, or where the data subject would be very angry.

For data files falling into class (A), it is appropriate to ensure that it is protected by a password. If the data is held on a microcomputer without password protection facilities, then the guidelines for microcomputers (see section 4) should be consulted. For a data file in class (B), the user should consider whether more stringent security precautions should be taken, such as, for example, encrypting the data, or separating data subject identification details from the other data subject information.

It is important to note that personal data in the public domain falls under the terms of the Data Protection Act if used in computerised form. In some instances, the merging of publicly available data about individuals may result in a combination of data which is regarded as sensitive by the data subjects. Consideration of the two questions above may be helpful in forming judgements in such instances.

If users are unclear about the level of sensitivity of their data, or what degree of security controls to apply to it, the University Data Protection Officer should be consulted.

(c) File Archives

Personal data files should be protected against loss or damage by taking copies of the files at appropriate intervals.

(d) Transaction Data

Any personal data held in intermediate files, prior to updating the main file(s), should be given the same level of access protection as the main file(s) and should be deleted from the computer (or put into archive) once the update process is complete.

7. Data Preparation

If it is intended to make use of a data preparation service to prepare personal data, then the management of that service should be consulted to agree any security procedures which may be required during the data preparation process.

Approved by the University Court July 1985

Reprinted with minor alterations November 1986

Appendix: Local Measures to Conform to the Code of Practice for Security of Computer-based Personal Data Files

General

Before you become a user of ERCC, you have to sign the *Regulations for Use* form which, inter alia, requires you to adhere to the Data Protection Act.

Section 2: Passwords

Some systems, including EMAS, have a third level of password – the transfer password, which is used to control access to a process for certain file and information transfer purposes. You should change your transfer password at the same time as you change your other passwords.

Section 3: Printed Output

Users who wish to supervise their output being printed should contact Job Reception. Users who have sensitive data to print and wish to use ERCC printers should list their files to LP23 (ERCC, KB) or LP25 (Appleton Tower) and at the same time put them in a forms queue. The forms queue for sensitive data using normal listing paper is 100 and for special paper requirements the existing forms queue plus 100 should be used (for example to print labels with sensitive data on LP25 list your file to .LP25,,126)

The output racks at Job Reception are not secure areas and sensitive data should not be left in them.

All output listed by ERCC under the sensitive data forms queues will be retained in a secure cabinet at the appropriate Job Reception or returned to the user in a sealed envelope.

Section 3: Disposal of Printouts

The University provides a service for the shredding of confidential waste paper. Information about the service is available from Mr A.B.Alison, Services Manager, 56 Buccleuch Street (031-667 1011 ext. 6300).

Section 6: Data Files

On EMAS 2900 three commands are accessible via directory PLULIB.PACKDIR to improve the security of text files. ENCRYPT and DECRYPT encrypt and decrypt the contents of text files, and WIPEFILE overwrites the contents of a text file with blanks before destroying it.

Section 7: Data Preparation

All data handled by the Data Preparation Service is treated in confidence. If you have sensitive data, you should arrange with the Data Preparation Supervisor to deliver directly to her, and collect directly from her all your input data. Keyed data is placed in an EMAS file of your choosing; thereafter you should handle it as described in Section 6.

Further Advice

If you wish further advice on interpretation of the Data Protection Act, or on deciding whether it applies to your data then you should consult either your departmental Data Protection Officer or the University Data Protection Officer, Mr D.J.Cronin, Secretary's Office, Old College (031-667 1011 ext. 4218).

Once you have determined that you have data which is personal, you may wish assistance with the computer procedures recommended in the Code for looking after it properly. For such technical guidance, you should contact the ERCC Advisory service (031-667 1011 ext. 2300 or 031-667 1081 ext. 2976).

ERCC November 1986