

1 4 9 5



**UNIVERSITY  
OF ABERDEEN**

**COLLEGE OF LIFE SCIENCES & MEDICINE**

**CONFIDENTIALITY  
GUIDELINES**

# CONTENTS

CONTENTS .....	2
1. INTRODUCTION.....	3
1.1 General Introduction .....	3
1.2 Confidential Information.....	3
1.3 Data Protection Act 1998.....	4
2. CARE OF DATA.....	5
2.1 Handling of Data.....	5
2.2 Data Security.....	5
2.3 Disposal of Confidential Data.....	5
2.4 IT Security .....	5
3. RELEASE OF DATA .....	6
3.1 Within the College of Life Sciences & Medicine .....	6
3.2 Outwith the College of Life Sciences & Medicine .....	6
4. APPENDIX A - Confidentiality Guidelines .....	7

# 1. INTRODUCTION

## 1.1 General Introduction

All permanent and temporary members of staff and students working in, or attached to, the College of Life Sciences & Medicine may have access to confidential information relating to individuals, including members of the general public, patients, other students or staff members. The information may be in textual, computerised, audio / video-taped or other form. It is of the utmost importance that personal information, which would not normally be generally available to others, is treated in an appropriate confidential manner. This is formalized in the Statement of Particulars of Terms & Conditions of Employment. Failure to follow the confidentiality guidelines jeopardises the credibility of the College and may lead the University to breach legal requirements such as the Data Protection Act. In the case of research projects, lapses in confidentiality may breach written assurances made on behalf of the College to the Ethical Committees of Aberdeen University, Grampian NHS Board and NHS Trusts.

The College of Life Sciences & Medicine is committed to ensuring that all personal data, in whatever form, which is collected and held under its auspices, are dealt with in an ethical and legally responsible manner. In order to ensure that staff and students meet this commitment, the College's confidentiality guidelines are outlined in this document.

## 1.2 Confidential Information

### **Confidential Data**

Data which is not in the public domain and which may also relate directly or indirectly to an individual. This would also include data that are subject to any duty of confidence. Statistical data which are not identifiable to individuals, but are considered sensitive, should also be considered as confidential data.

### **Personal Data**

Data or information relating to a named or identifiable individual, in any form (computer, manual, textual, email, sound or image data).

### **Data Subject**

The individual on whom personal data are held.

### **Identifiable Data**

Data, other than named, which can be directly or indirectly linked to an individual or where the individual's identity may be inferred (e.g. by linking two data items which would not in themselves be regarded as sensitive, for example postcode plus date of birth).

Individuals may be identified by Name, personal identifier (e.g. CHI Number, Case Reference Number, NHS Number, GMC Number, Staff Number), Postcode. Statistics

used for a small sample size may also be used to infer an individual's identity from other less obvious data items.

### **Anonymised Data**

Data on individuals which are not identified and not identifiable.

## **1.3 Data Protection Act 1998**

The Data Protection Act 1998 legislated specifically on the treatment and use of confidential data held in a structured way in any medium (paper, computer, microfiche, tape, etc). General Guidelines are listed in **Appendix A**.

Any clinical / medical data must be treated with particular care and protected from unauthorised access. Care should be taken with anonymised data sets to ensure that there is no potential for unauthorised identification, especially for small data sets where identification could be implied. A named clinician must be identified to take responsibility for the data security; preferably the doctor who takes clinical responsibility for the patients, otherwise one of the medically-qualified staff members at consultant level within the College of Life Sciences & Medicine. Potentially identifiable clinical data must be stored under lock and key.

As a last resort, the Head of College reserves the right to destroy any data, in any form which are considered to be no longer of value or which place the College in breach of the Data Protection Act or any other pertinent guidelines or legislation.

Advice on confidentiality, for current data held or planned for the future, can be obtained from line managers or project supervisors in the first instance; otherwise, the confidentiality co-ordinator (Mrs Val Angus, Email: [v.angus@abdn.ac.uk](mailto:v.angus@abdn.ac.uk)) will be pleased to advise.

The University's compliance with the terms of the Data Protection Act can be accessed using the link [www.abdn.ac.uk/dataprotection/](http://www.abdn.ac.uk/dataprotection/)

The University is registered on the Information Commissioner's Office web site <http://www.ico.gov.uk/ESDWebPages/search.asp> Registration Number Z7266585, which describes personal data being processed.

## 2. CARE OF DATA

### 2.1 Handling of Data

It is each person's responsibility to ensure that the data they are working on are not read or handled by anyone who has no need to do so. In the event that confidential data is lost or even suspected to be lost, the Confidentiality Co-ordinator (Mrs Val Angus) should be notified immediately.

Confidential information should not be discussed in a public place and copies of confidential information should be kept to a minimum.

### 2.2 Data Security

It is each person's responsibility to ensure the physical security of the documents and / or media that they use, including storage of files on PCs.

Confidential information must never be left unlocked in an unattended room and should be locked away when not in use. PCs should be password protected, unless they are physically locked in an office for short periods of absence or powered down when unattended.

### 2.3 Disposal of Confidential Data

Confidential data can be disposed of in designated "confidential paper shredding & recycling" bins, which are kept secure until controlled disposal is arranged.

Floppy disks and CDs containing confidential information to be erased must be re-formatted before re-use.

### 2.4 IT Security

Staff and students have a unique username and password for access to the relevant portion of the University's Local Area Network (LAN). Additional levels of security exist for access to confidential systems.

User passwords must not be written down or disclosed to other individuals. Passwords should be a combination of numbers and uppercase and lowercase characters.

### 3. RELEASE OF DATA

#### 3.1 Within the College of Life Sciences & Medicine

Confidential information must be made available only to other authorised individuals who need to know. Information may be passed directly by hand or in a sealed envelope marked **CONFIDENTIAL** .

E-mail must not be used to transmit confidential information, unless the data files are encrypted and password protected. Under no circumstances should confidential information be published on the World Wide Web or communicated over the Internet.

#### 3.2 Outwith the College of Life Sciences & Medicine

Confidential data must only be disclosed to authorised individuals on the understanding that they are used only for the purposes specified.

E-mail must not be used to transmit confidential information, unless the data files are encrypted and password protected and similarly, identifiable confidential information must not be disclosed by telephone or by FAX. Under no circumstances should confidential information be published on the World Wide Web or communicated over the Internet.

Personally-identifiable data must not be used as part of presentations. Anonymised data must be used for this purpose.

Confidential information must be transported by recorded delivery or Securicor in sealed double wrapped envelopes, the inner envelope only should be marked **CONFIDENTIAL** and the outer envelope should contain the name and address of the recipient.

#### 4. APPENDIX A – Confidentiality Guidelines

1. Where it is possible, you should obtain full informed consent for collection and processing of all data provided by individuals. Where this is not possible, you must obtain the consent of the appropriate ethics committee before collecting the data.
2. You must respect the privacy of individuals on whom you have access to personal data.
3. You must not divulge to anyone else personal information which is not normally in the public domain without the explicit consent of the data subject.
4. You will be held responsible for all aspects of obtaining, storing, protecting, processing and reporting of personal data collected by you or on your behalf.
5. You may only obtain personal information in a fair and lawful manner.
6. You may only hold and use personal data for specified and lawful purposes.
7. All personal data you hold should be adequate, relevant and not excessive in relation to the purpose or purposes for which it is collected.
8. You must take steps to ensure that personal data you hold is accurate and, where necessary, kept up to date.
9. You may not hold personal data for longer than is necessary for the specified purpose or purposes. You may continue to hold the data only if it is rendered completely and permanently anonymous.
10. If he or she requests it, you must be prepared and able to provide to any individual for whom you hold personal data, confirmation that he or she is a data subject and a copy of the relevant data which you possess in an identifiable format.
11. You must be prepared to correct or erase personal data if the data subject can demonstrate that the data you hold are inaccurate or incorrect.
12. You must take appropriate security measures to protect personal data against unauthorised or accidental access, alteration, disclosure, destruction or loss.
13. In cases of disagreement, dispute or uncertainty regarding personal data, you must seek the advice of the College's Confidentiality Co-ordinator or the Head of College.
14. You should carefully consider the implications of sharing information about planned or ongoing research projects to third parties, especially (but not exclusively) representatives of the media. The publication of details of a research project involving the general public in the press, radio or television may undermine the methodology and invalidate ethical approval.