

HOSPITAL RADIO PERTH

DATA PROTECTION

ONE **DEFINITIONS**

In this document

The term "Organisation" will refer to Hospital Radio Perth.

The term "Data Controller" will refer to the Organisation in its capacity to record and use personal information.

The term "Committee" will refer to the managing committee of Hospital Radio Perth.

The term "Member" will refer to any full, associate or probationary member of Hospital Radio Perth.

The term "Data Subject" will refer to any Member or any other identifiable living individual whose personal data is held by the organisation.

The term "The Act" will refer to The Data Protection Act 1998

The term "FOIA" will refer to the Freedom of Information Act 2000

The term "FOISA" will refer to The Freedom of Information (Scotland) Act 2002

TWO **THE DATA PROTECTION ACT 1998**

The Act works in two ways:

- a) It says that anyone who records and uses personal information (data controllers) must be open about how the information is used and must follow eight principles of good information handling.
- b) It also gives us all as individuals (data subjects) certain rights, including the right to see information that is held about us and to have it corrected if it is wrong.

THREE **THE PRINCIPLES OF GOOD INFORMATION HANDLING**

All data controllers must follow the eight data protection principles. They say that data must be:

- a) Fairly and lawfully processed;
- b) Processed for limited purposes;
- c) Adequate, relevant and not excessive;
- d) Accurate and up to date;
- e) Not kept for longer than is necessary;
- f) Processed in line with the data subject's rights;
- g) Held and maintained in a secure manner;
- h) Not transferred to countries outside the EU without adequate protection.

FOUR **CONFIDENTIALITY**

In the interests of confidentiality, the Organisation shall limit the number of Members who may process data. They shall normally be members of the Committee of the Organisation.

Those individuals who process such data, shall be responsible for its security and maintenance.

They must pass this data over to any other named Member or delete or destroy the data forthwith, when required so to do by the Committee.

FIVE **ENFORCEMENT**

The Information Commissioner enforces and oversees the Data Protection Act 1998 and the Freedom of Information Act 2000. In Scotland, however, the Freedom of Information Act 2000 has no jurisdiction and is regulated by the office of the Scottish Information Commissioner under devolved legislation, the Freedom of Information (Scotland) Act 2002. Whilst the Organisation is not incorporated under the Act, all NHS Trusts are and therefore the Organisation may be required to respond to a request made to NHS Tayside Trust.

HOSPITAL RADIO PERTH

DATA PROTECTION

The Commissioner maintains a public register of data controllers. Notification is the process by which a data controller's processing details are added to the register. Under the Data Protection Act every data controller needs to notify unless they are exempt.

Even if you are exempt from notification, best practice says that you must still comply with the principles.

SIX **EXEMPTION FROM NOTIFICATION**

As a not for profit organisation Hospital Radio Perth has no requirement to notify. The Organisation is exempt, provided all of its processing conforms to the following guidelines:

- a) The processing is only for the purposes of establishing or maintaining membership or support for a body or association not established or conducted for profit, or providing or administering activities for individuals who are either members of the body or association or have regular contact with it.
- b) The data subjects are restricted to any person the processing of whose personal data is necessary for this exempt purpose.
- c) The data classes are restricted to data which is necessary for this exempt purpose.
- d) Disclosures other than those made with the consent of the data subjects are restricted to those third parties which are necessary for this exempt purpose.
- e) Personal data is not kept after the relationship between the organisation and the data subject ends, unless and for so long as it is necessary to do so for the exempt purpose.

SEVEN **THE RIGHT OF SUBJECT ACCESS**

Under the Data Protection Act individuals can see the information about themselves that is held on computer and in some paper records. This is known as the right of subject access.

If the Organisation receives a subject access request then the individual must be sent:

- a) A copy of the information held on them;
- b) A description of why this information is processed;
- c) Details of anyone it may be passed to or seen by; and
- d) The logic involved in any automated decisions.

A subject access request must be dealt with within 40 days from the date of receipt of the request in writing from the person whose information is being requested or their authorised representative. If further details are required from the person making the request to help find the data, or in order to confirm their identity, the 40 days will begin on receipt of this extra information.

A statutory fee of £10 will be levied for responding to such a request and the 40 days will not begin until both the written request and payment are received.

Individuals making a subject access request will be given a redacted copy of the information held about them, both on computer and specific paper records.

They will be furnished with a description of why their information is being processed, anyone it may be passed to, and where the data came from. The information will be provided in an easy to understand format and any codes used must be explained.

EIGHT **PROCESSING SENSITIVE DATA**

The Organisation operates an Equal Opportunities Programme however, the Organisation will not

HOSPITAL RADIO PERTH

DATA PROTECTION

process sensitive personal data which is defined in the Act as: racial or ethnic origin; political opinions; religious or other beliefs; trade union membership; health; sex life; criminal proceedings or convictions, unless the Organisation:

- a) Has the explicit consent of the individual.
- b) Needs to process the information in order to protect the vital interests of the data subject or another.
- c) Is required to do so for legislative reasons.

NINE **OTHER RELEVANT POLICIES**

This Policy should be read in line with:

- The Computer, Email and Internet Policy
- The Retention Policy

Data Protection

last amended 25 October 2011