

## INTRODUCTION

The Data Protection Act 1998 act was fully implemented in 2001 and replaces all previous legislation regarding the processing of personal data. The act is valid for the whole of the United Kingdom.

As with any legislation covering personal data there has been a great deal of suspicion and misapprehension of the scope of the act, and many see it as a further restriction of civil liberties. In real terms exactly the opposite is true. The Data Protection Act 1998 imposes a responsibility on any individual or organisation who need to collect data on any living persons to consider very carefully how they do so, and has established a legal framework to ensure that not only all parties comply with the act but that any contravention can be dealt with in court.

This is designed to offer legal protection to everyone who has supplied data on themselves and to guarantee that the data is processed fairly and not misused or passed on to other bodies without consent.

The act in its simplest form covers personal data on any living individuals – this encompasses how we collect the information, the range of data we collect, how it is transferred, how it is stored and how long we need to retain it. There is also an obligation to notify those supplying the data of exactly why it is being collected and who has access to use it. Most importantly any member of the relevant organisation is now empowered to formally request to know what data is being held on them.

The Freedom Of Information Act 2000 is a piece of legislation which allows an individual member of an organisation to make a formal request on payment of an agreed fee to access all the information held on them by that organisation, including all computer and paper records, e-mails etc. These requests must by law be processed within 20 working days.

## WHAT IS PERSONAL DATA?

Personal data is defined as information we process about “living identifiable individuals”. Processing is how we record, store, organise, adapt, alter, retrieve, share and delete the information. The type of data can include:-

- Computer records (floppy disks, CD, DVD, hard disks, back up files)
- Audio and video files including CCTV, digital media, scanned images etc.
- Manual files ( written and typed records, card index systems, microfiche records)
- E-Mails, web records etc.

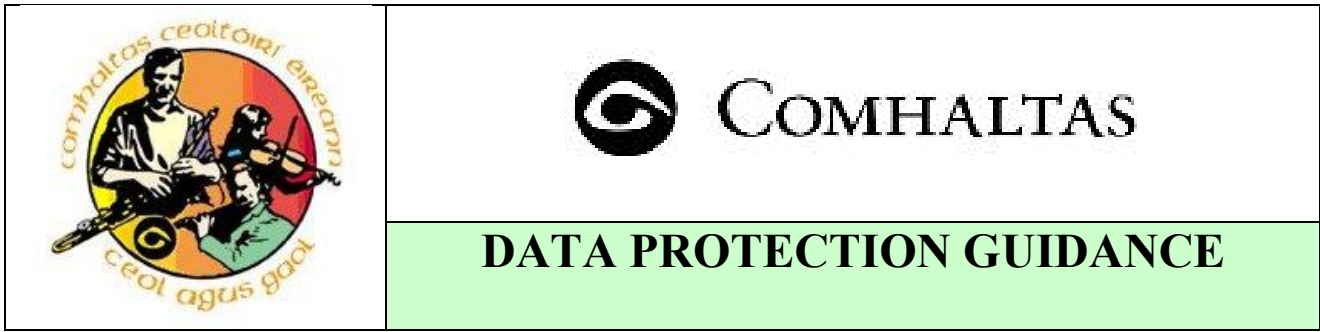
## **EXEMPTIONS**

There are various exemptions to data held where the information is deemed “sensitive”. This mainly covers areas of medical, police, legal and security records which we are unlikely to require in CCE.

## **RESPONSIBILITY**

The Data Protection Act 1998 provides a structure for each organisation to adopt in order for the implementation of data protection procedures to take place. These procedures must be adopted throughout the organisation from Provincial to regional and branch level including any ad hoc committees.

Where every effort will be made to make staff and volunteers aware of the correct code of practice in handling personal data it must be stressed that unlike Child Protection there is no corporate responsibility - the onus is on the individual members to ensure that data is not lost, made public or passed on to any third party agencies without prior approval. Any breach of security or confidentiality can result in a fine to the individual of up to £5,000.



## 1. POLICY STATEMENT

1.1 The confidentiality and security of any data provided to support any Comhaltas activities must be safeguarded at all costs. Members have a right to know that as an organisation we will take all appropriate measures to protect any personal data that has been provided.

1.2 Comhaltas will adopt a formal data protection policy and will ensure it is implemented in full

1.3 Comhaltas recognises that data protection policies and procedures are of benefit to staff and volunteers as increased awareness of security issues will help prevent accidental disclosure of data and subsequent action.

## 2. AIMS AND OBJECTIVES

This policy ensures that all workers and volunteers are aware of the eight data protection principles. All data must be :-

1. Processed fairly and lawfully
2. Obtained only for one or more specified and lawful purpose
3. Adequate, relevant and not excessive
4. Accurate and kept up to date
5. Kept no longer than is necessary for the lawful purpose
6. Kept in accordance with the rights of the individual
7. Stored using appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or damage
8. Retained within member countries of the European Economic Area

## 3. IT IS COMHALTAS POLICY THAT :

1.1 Persons within the organisation responsible for collecting or processing data will take appropriate action to ensure security and confidentiality at all times

1.2 Personal details must be collected through formal designated processes

1.3 The collection of personal data must be restricted to the minimum required for official processes

1.4 A statement should be made available to those from whom data is collected in the form of a Fair Processing Notice, which explains what personal data is collected and processed, the reason it is required to be collected and who is formally granted access to that information.

1.5 All personal data must be accurate and regularly updated

1.6 Records relating to those who cease to be members should be retained for a period agreed by the Provincial Council and then deleted or destroyed.

1.7 Whether records are stored on paper or electronically all appropriate measures must be taken to protect the data from unauthorised use or access, loss or damage. Where necessary a secure backup copy of the data should be available in case of accidental loss or damage.

#### **4. MONITORING AND REVIEW**

The Provincial Council will review this policy regularly and provide effective management and training



COMHALTAS

## DATA PROTECTION GUIDANCE

### CODE OF PRACTICE

Comhaltas workers and volunteers should take the following steps to protect and secure the data which they hold regardless of the format, quantity or number of people who may assist in its processing.

#### COMPUTERS:-

- Use passwords / lock the computer screen
- If networked use a secure drive
- Download Windows updates - most contain added security against vulnerabilities
- Install Anti Virus / Anti Spyware software - these prevent third parties accessing your data online
- Clear recent documents and temporary files ( use free software from <http://www.ccleaner.com/>)
- Clear your printer and shred unwanted copies
- Make backups of your data in case of computer failure - store in a different secure location
- Make sure laptop computers are locked away when not in use
- Provide secure locked storage for portable media such as floppy disks, CDs, DVDs and memory sticks

#### MANUAL RECORDS:-

- Paper records should be kept in a structured filing system to ensure all data can be located if requested under the freedom of information legislation
- Any such records should be kept in a secure environment - rooms / cupboards that can be locked
- Check no spare copies are left in copiers, fax machines or scanners etc
- All old paper records should be shredded before disposal

#### MAIL:

- Any personal details should only be posted when the recipient is authorised to use the data
- The envelope must be clearly marked to the named recipient and labelled as confidential.
- A return address should always be provided in case the mail is not delivered

#### E-MAIL:

- Always ensure the correct recipient is used in the address before sending - often one letter or full stop is enough to send the message to a completely different person
- If a message is accidentally sent to the wrong person it must be recalled immediately
- Never include personal data in the subject line of an e-mail

- Unless the recipient is known do not send personal data at all, but even when known try and prevent identification to external users by using initials or reference numbers.
- Only print off e-mails containing data if absolutely necessary
- Never copy personal data directly into the body of an e-mail. You can enter a list of names but no identifiers such as dates of birth or addresses. If this is needed use a secure attachment ie Excel spreadsheet.
- If attaching a spreadsheet make sure it is password protected. The recipient can be given the password by phone or in another message.. (To password protect a spreadsheet open the file and select "Save As" then when you have the dialog box displayed select "Tools" then "General Options" - you can enter a password to open before saving).

## **PHOTOGRAPHS / VIDEOS**

- Photographs or video films taken by parents, grandparents, friends or other family are not subject to the data protection legislation where the use is entirely personal for family albums or home display.
- If the photographs or films are to be used by Comhaltas in publications or archive films the data protection act will not normally apply providing that the organisation had agreed in advance to the filming and that the children and parents were made aware that the filming may take place in advance.
- If photographs are taken at competitions by the press it is not necessary to get separate parental permission if participants were notified in the programme or pre event publicity that photographs were expected to be used by the press in this context unless any objections were lodged in advance

## **DEFINITIONS**

**Data Controller** – the individual or organisation, ie CCE

**Data User** – any CCE member processing the data on behalf of the organisation

**Data Processor** – any third party processing data on behalf of CCE

**Data Subject** – any individual on whom information is held

**Information Commissioner** – the government department responsible for data protection