

# **The Data Protection Act 1998**

## **Guidance Notes for the Free Church of Scotland**

The Data Protection Act 1998 gives individuals who are the subject of personal data, certain rights including the right to know what information (data) is held about them by all organisations who handle personal information. “Data”, as defined in the Act, is, generally speaking, information held on a computer system or as part of a manual filing system. The Act also requires such organisations to hold, or process, information in a certain way and in accordance with certain principles. These notes are a brief guide as to how the Church as a whole and also individual congregations may be affected by the Act and in particular how information should be processed by the Church and by its individual congregations.

### **Data Protection Principles**

The Act sets out 8 data protection principles which should be followed in respect of personal data. “Personal data”, as defined in the Act, means data which relate to a living individual (defined in the Act as a “data subject”) who can be identified from those data or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, eg. the Church. The basic principles are:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be processed in a manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for any longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

It will usually be obvious what is or is not personal data. The Information Commissioner’s Office website, [www.ico.gov.uk](http://www.ico.gov.uk), contains a lot of useful information on all aspects of data protection, including a guidance note entitled “What is personal data? – A quick reference guide”, to assist in determining whether data falls within the Act’s definition of personal data in situations where this is not obvious. A more in depth guidance note, “Determining what is personal data” is also available.

The Act also effectively creates a new category of “sensitive personal data”, defined in the Act as meaning personal data consisting of information as to:

- a) the racial or ethnic origin of the data subject,
- b) his political opinions
- c) his religious beliefs or other beliefs of a similar nature
- d) whether he is a member of a trade union
- e) his physical or mental health or condition
- f) his sexual life
- g) the commission or alleged commission by him of any offence, or
- h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

In order for an organisation to hold “sensitive personal data” legally, it must usually have the express consent of the individual. Sensitive personal data may also be lawfully processed, for example, if the processing is carried out as part of the legitimate activities of a not-for-profit body or association, such as the Church. In order to take advantage of this condition the processing must:

- a) be carried out with appropriate safeguards for the rights and freedoms of data subjects,
- b) relate only to individuals who are either members of the body or association or have regular contact with it in connection with its purposes, and
- c) not involve disclosure of the personal data to a third party without the consent of the data subject.

## **Purposes for which the Church keeps personal data**

The Church keeps personal data about individuals for various purposes, including:

- Staff Administration (including volunteer staff, eg. those working with children and young people)
- Administration of Membership Records
- Fundraising
- Realising the Objectives of the Church as a Charitable Organisation
- Pastoral Care
- Education

## **Examples of the sort of personal data held by the Church**

Basic information will be held, such as staff/payroll records; membership lists; baptismal records; information regarding those attending camps or other activities; lists of children attending Sunday Schools; records of those for whom the Church holds contact details for various reasons, including volunteers working with children and young people and others, those attending churches, making Gift Aid donations etc. These are examples only and there may be other types of personal data held.

## **The duty to keep personal data secure and confidential**

The Act requires all organisations to have appropriate security to protect personal information against unlawful or unauthorised use or disclosure, and accidental loss, destruction or damage. Data should be kept on secure computer systems and/or in secure manual filing systems. In particular:

- passwords should be kept secure, should be changed regularly and not shared.
- if computers are in shared areas the user should lock or log off when away from his or her desk.
- confidential paper waste should be disposed off securely by shredding.
- in order to prevent virus attacks care should be taken when opening emails and attachments or visiting new websites.
- hard copy personal information should be securely stored and not visible when not being used.
- visitors should be signed in and out of premises, or accompanied in areas normally restricted to “staff”.
- computer screens should be positioned away from windows to prevent accidental disclosure of personal data.
- personal data being taken off the premises should be encrypted if it would cause damage or distress if lost or stolen.
- back-ups of data should be kept.

Clearly not all of the above will apply in certain situations and it is for individual congregations to decide which security measures are put in place in their particular situation, subject of course to them taking all measures necessary to ensure that they are complying with the Act.

The Church must respect the individual’s right to confidentiality. Care must be taken to ensure that third parties cannot access the data without the permission of the individual concerned and that data about individuals is not disclosed – to third parties or others – without their consent, unless the Church is allowed or obliged to disclose the data by law.

In particular care should be taken in dealing with any request for information over the telephone. The amount of information given out over the telephone should be limited and in any event identity checks should be carried out if giving information out over the telephone, whether by way of an incoming or an outgoing call, to ensure that the person requesting the information is either the individual concerned or someone properly authorised to act on their behalf.

## **To keep or destroy records?**

Records should be kept as long as necessary – the length of time records are kept depends on the type of data held in the records and the Act does not specify what a “necessary” period should be for particular information. If there is no legal requirement to keep personal data, it should be destroyed as soon as it is no longer required and it is practicable to do so. Data processors should be able to give a good reason for retaining/processing data.

## **Sharing of data**

The Church should obtain the consent of the individual concerned before passing personal information on to a third party, unless it is allowed to share the information by law. It is therefore always safest to ensure that you have the consent of the individual to allow you to share data with third parties. As a result, every form used to collect data should contain:

- information as to how the personal data will be used
- details of third parties (if any) with whom the personal data will be shared
- a declaration by the individual that he/she consents to the data being used for the stated purposes.

## **Rights of individuals**

The Act gives individuals a number of rights, including the right:

- to be given a description of the personal data held about them in computer or manual record systems,
- to be given a description of any information available to the data controller (the Church) as to the source of those data
- to be given a description of the purposes for which the personal data are being or are to be processed,
- to be given a description of the recipients or classes of recipients (if any) to whom they are or may be disclosed, and
- to have inaccurate data corrected within 21 days of an individual being given access to the data.

In some cases it will not be possible to comply with a request for information without disclosing information relating to another individual who can be identified from the information requested. In this event the data controller *may* be entitled to refuse to give the information. If complying with such a request would involve disclosing information regarding another individual, advice should be sought from the Free Church Offices before proceeding further.

## **Handling requests from individuals to see personal data held about them (known as subject access requests)**

A request for information must be made in writing. Once such a request has been received a response must be made within 40 days of receiving:

- the written request,
- proof of identity. It is important to ensure that the person making the request is who they say they are. Accordingly, unless the identity is beyond doubt, identification documents such as a passport or driving licence should be requested, and

- any additional information necessary to locate the individual's records.
- payment of any fee (the maximum amount that can be charged is £10).

The individual should be given a copy of the data contained in the files. Where providing a copy of the data would involve disproportionate effort, then the individual should be invited to view the material. Depending on the sensitivity of the data, consideration should be given as to whether it should be delivered personally or sent by special or recorded delivery.

It is recommended that the Free Church Offices be contacted in the event of a data subject request being received.

### **Requests by individuals for data about members of their family or about any other person**

Individuals are not entitled to see data about third parties, including data about members of their family, unless the third party has either given their consent in writing or it is reasonable to proceed without obtaining their consent. Parents *may* be provided with data about their child, depending on the age and wishes of the child and provided that the parent has parental responsibilities and rights. The age of legal capacity in Scotland is, generally speaking, 16. Where a question falls to be determined as to the legal capacity of anyone under the age of 16 to exercise any right conferred by the Act, that person shall be taken to have that capacity where s/he has a general understanding of what it means to exercise that right, and a child aged 12 or more is presumed to be of sufficient age and maturity to have such an understanding. In certain circumstances (for example if someone is a member of an elderly person's family) a person may have been granted powers to see data about that family member by way of a Power of Attorney or Guardianship Order. In these situations a check should be made that the permissions/authorisations are genuine before giving out data.

### **Other rights of individuals under the Data Protection Act 1998**

In addition to those described above, these are some of the other rights individuals have:

- to prevent processing of personal data which is likely to cause damage or distress.
- to prevent the processing of personal data for the purposes of direct marketing.
- to ask for compensation if they have suffered damage as a result of a breach of the Act.
- to ask the Information Commissioner to investigate to see if there has been a breach of the Act.

Courts will only support a claim for compensation by an individual if they can show that an organisation had not taken reasonable care to ensure that it complied with the relevant requirement of the Act.

An individual can complain to the Commissioner if they consider that an organisation has breached any of the requirements of the Data Protection Act. This includes a breach of any of the data protection principles, a failure to respond to any written

notices, processing data without the individual's consent (where consent is necessary) and refusing to provide the individual with the personal data requested by them. This list is not exhaustive.

It is very important to remember that if the Church breaches any provision of the Act, it can be fined. It is also possible for the Information Commissioner to ask for criminal proceedings to be raised against the Church. All congregations must therefore be aware of their duties under the Act and must comply with them.

At the request of an individual, the Commissioner can carry out an assessment of an organisation's processing to establish whether or not it is acting in compliance with the Act.

Should the Commissioner decide that an organisation is breaching the Act, then it will issue a notice requiring steps to be taken to ensure compliance.

**To summarise**, the Act gives individuals the right to know what information is held about them by organisations and sets out 8 principles for the proper handling of that information. The following checklist of questions for those within the Church who are processing data to ask themselves should give an indication as to whether they are complying with legal obligations of the Church under the Act:

- Do we really need this information about an individual and do we know what we are going to use it for?
- Do the individuals about whom we hold information know that we are holding it and are they likely to understand what it will be used for?
- If we are asked to pass on personal information, would the individuals about whom it is held expect us to pass it on?
- Are we satisfied that personal information is being held securely, whether on computer or on paper?
- Is access to personal information limited to those who "need to know" it?
- Is all personal information held by us accurate and kept updated?
- Do we delete or destroy personal information as soon as we no longer actually need it?

Finally, these Notes are intended to give general guidance only. Advice in respect of specific situations can, if required, be obtained from the Free Church Offices who will be happy to assist.