

1 The Data Protection Act has been extended and now covers the keeping of all records both electronically and on paper.

2 Under the new legislation, the ruling of the past few years that *'local congregations of the United Reformed Church storing information on computer or disk and who are members of a Provincial (Synod) Trust need not register with the Data Protection Registrar (now called the Information Commissioner) providing that the Provincial (Synod) Trust has registered'* **NO LONGER APPLIES.** However for most local churches the observance of principles of fair practice will mean that there will be no **need to register individually.** To comply with the Data Protection Legislation the following principles must be met and these apply to all those holding data **in any form whatever.**

All processing of personal data must be fair and should meet the following conditions:

- the person concerned (the data subject) has given consent - or is being used;
- to carry out a contract to which that person subject is a party;
- to meet a legal obligation of the data controller (i.e. the person responsible for the keeping of the record);
- to protect the vital interests of the person concerned;
- for various judicial and government functions;
- in the legitimate interest of data controller (unless it causes harm to the rights, freedom or legitimate interests of the person concerned).

Personal data can only be collected and used for specified purpose(s).

- The data must be adequate, relevant and not excessive.
- The data must be accurate and up to date.
- The data must not be held longer than necessary.
- The data subject's rights must be respected.
- You must have appropriate security.

Please note – special rules apply to the transfer of data abroad and are not dealt with in this note of guidance.

### **3 What to do to ensure your church complies with the legislation Draw up a policy**

This policy statement should cover such items as:

- why the information is to be held including any secondary use that will be made of it;
- what kind of information is to be held;
- whether any information is being collected without the knowledge of the person concerned;
- what types of disclosure that are likely to be made;
- how you intend to ensure that the information held is accurate;
- how long will need to keep the information;
- what level of confidentiality will be applied;
- any special security measures that apply.

### **4 Ensure those who have access to the data know exactly what they are allowed to do with people's information**

**5 Ensure anyone about whom you hold information knows it is held, what it is used for and to whom you might pass it on.**

**6 Get consent wherever possible for holding people's information and obtain explicit consent in writing if any detail could be classified as sensitive. The definition of 'Sensitive information' includes racial or ethnic origin, religious or political beliefs, Trade Union membership, health, sex-life or criminal record.**

**7 Make sure people are offered the chance to opt out of receiving any direct mailing, including fund raising. Design or modify your system so anyone may have access to their own record without being able to view others records. Make appropriate security arrangements for both manual and computer systems – as a minimum these should include passwords for computer systems and secure storage for manual records. Archive or delete records regularly.**

**8 A brief guide for those handling personal data:**

- when you hold personal data remember;
- it can only be used for the purposes for which it was originally obtained;
- you have to take good care of it;
- you have to use it fairly;
- you must ensure that it is adequate, relevant, not excessive, accurate, up to date and not being held longer than necessary;
- you are committing an offence if you get access to personal data you are not authorised to see, or if you disclose such data to other people;
- you are committing an offence if you sell personal data you are not entitled to.

**9 When you obtain personal data remember:**

- you must not deceive or mislead anyone;
- you must ensure the person concerned knows you are collecting the data and why and how it may be used;
- if data is proved from someone other than the individual concerned (the DATA SUBJECT) you must ensure the Data Subject knows you are using their data and why and how it will be used;
- you may have to get consent from the Data Subject to use their data, particularly if it is in any of the sensitive areas of racial or ethnic origin, religious or political beliefs, Trade Union membership, health, sex-life or criminal record.

**10 When you disclose personal data remember:**

- you must check that the disclosure fits the purpose(s) for which the data is being held;
- you must check that the person you are disclosing it to is authorised to have it;
- you must check that the Data Subject is aware that this type of disclosure is possible or that there is an overriding reason, such as a legal obligation;
- if you put personal data on the WEB you will need consent from the data subject.

**11 Data subjects have rights too:**

- data can only be used if consent is given- but you can explain the consequences of withholding it;
- data cannot be used for direct mailing of any goods or services if the person concerned has refused permission;
- if you are telephoning people at home for direct marketing purposes you must check the number you are calling is not on a barred number register;
- data subjects can ask to see ALL the personal data you hold on them, including manual files.

12 The Legal and Trust Officer holds a Data Protection Handbook at the Synod Office, entitled, **A complete guide to notification. The document** includes the following sections:

- The notification life cycle;
- Completing the notification form;
- The Part 2 the Form;
- Completing the form on the internet;
- Notification exemptions;
- Changes introduced by notification;
- Glossary of terms.
- 

**The information contained in this guideline has been extracted from the URC Communications and Editorial Committee' booklet – The Data Protection Act and the Handbook mentioned above.**