DATA PROTECTION

A Guidance Note for Church of Scotland Congregations

Data

The Act contains a number of defined terms. Personal Data is classed as any information relating to an identifiable living individual (i.e. a Data Subject).

The category of Sensitive Personal Data consists of information relating to:

- the racial or ethnic origin of the data subject
- their political opinions
- **their religious or other beliefs of a similar nature**
- whether they are a member of a trade union
- their physical or mental health or condition
- their sexual life
- the commission or alleged commission by them of any offence, or
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

'Religious or similar beliefs' is in bold because a significant amount of Personal Data held within the Church of Scotland environment will actually be Sensitive Personal Data. The mere holding of any information about a particular person by a Church of Scotland congregation could be indicative of that person's religious beliefs. You should therefore be to be extra vigilant when dealing with any Personal Data.

Sensitive Personal Data has a higher level of protection afforded to it and can only be processed under strict conditions including the express permission of the person concerned (unless a specific exemption applies). As a result, if Personal Data is collected, stored or transmitted, appropriate steps will need to be taken to ensure that explicit consent to hold, use and retain this information has been made.

Notification

In general, any person or organisation processing or handling Personal Data electronically must notify the Information Commissioner unless that data is processed by a person for the sole purpose of their personal, family or household affairs. The Data Protection Register, detailing all 'data controllers' and the category of information they process is available on the Information Commissioner's website:

http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

There are exemptions from the requirement to notify, including one to cover 'not for profit' organisations where data processing is limited to: establishing or maintaining support or providing or administering activities for individuals who are members of the body or have regular contact with it. This 'exempt purpose' is therefore intended

for small clubs, voluntary organisations, church administration and some charities. Processing staff administration, advertising, marketing and public relations is therefore permissible without the need for notification. As a result, if congregations are processing membership and financial records only, they are likely to be exempt from notification. Subjects such as parents who are not church members or attenders but whose children go to Sunday school or another youth organisation run by the congregation will fall within the category of being in 'regular contact with the organisation'.

However, there is still a requirement to adhere to the Data Protection Principles and the rules regarding subject access requests (see below). Furthermore, the Act also includes a list of activities which prevent the exemption operating, including the processing of data for the purposes of 'pastoral care'. As a result, any information stored in relation to one to one counselling or similar activities provided by a Minister will fall out-with the exemption.

Once you have established whether or not the congregation's data processing falls within the exemption, you must contact your Presbytery Clerk to advise. The established practice has been for Presbyteries to notify on behalf of themselves and the congregations within their bounds. As a result, congregations do not have to notify (but may do so, if felt appropriate).

The same will apply if your congregation wishes to start any new processing of an 'unusual' nature. 'Unusual' information could include databases or information about anything but common examples would be details of those involved with community projects that the congregation is involved in, such as the big issue or soup/food kitchens. Any procession of this nature should be discussed with the Presbytery Clerk before the processing is commenced.

A regular dialogue should be in operation with Presbytery on the issue of data protection as notification to the Information Commissioner is to be made annually.

The Data Protection Principles

The 1998 Act requires data controllers (persons who determine the purposes for which and how any personal data is processed) to be open about how the information is used and to follow eight data protection principles of good information handling. Data must be:

1. fairly and lawfully processed
2. obtained for specific and lawful purposes
3. adequate, relevant and not excessive
4. kept accurate and up to date
5. not kept longer than necessary
6. processed in accordance with the data subjects' rights
7. kept secure
8. not transferred to countries outside the European Economic Area without adequate protection.

These principles apply both to certain paper based records and those kept on computer.

Non-compliance or an unintentional breach of the above principles can result in enforcement action being taken by the Information Commissioner. The most common cause of a fine has been the loss of data through unencrypted laptops and USB drives being lost or stolen.

In January 2012, Midlothian Council was the first Scottish organisation to be fined (£140,000) by Information Commissioner for failing to protect child care data. More recently, the learning disability charity, Enable Scotland, has had to sign an undertaking promising to improve its data security after two unencrypted memory sticks and papers containing the personal details of around 100 individuals were stolen from an employee's home.

As a result, Charities, and indeed a substantial organisation like the Church of Scotland, cannot expect that a softer line will be taken. There is also a huge reputational risk associated with a breach.

Congregations must therefore assess all data stored and develop an action plan for managing data. The following list contains suggestions only and is not exhaustive:

- Electronic data must be protected by standard password procedures with the 'computer lock' facility in place when office bearers or employees are away from the desk/workstation where information is held;
  Computer workstations in administrative areas in church premises should be positioned so that they are not visible to casual observers;
- Personal data stored in manual form e.g. in files should be held where it is not readily accessible to those who do not have a legitimate reason to see it and (especially for sensitive personal data) should be in lockable storage, where appropriate;
- All ordered manual files and databases should be kept up to date and should have an archiving policy. Data no longer required must be regularly purged;
- If data is to be transferred through memory sticks, CD-ROMs or similar electronic formats then the secure handling of these devices must be ensured. No such device should be sent through the open post – a secure courier service must always be used. The recipient should be clearly stated. If data is sent via a courier the intended recipient must be made aware when to expect the data. The recipient must confirm safe receipt as soon as the data arrives. The sender is responsible for ensuring that the confirmation is received, and liaising with the courier service if there is any delay in the receipt of the data.
- Laptops and USB drives should have appropriate security and 'encryption'.
- Personal data must not be transmitted to an office bearer's home Personal Computer without appropriate assurances from him/her that the foregoing safeguards will be put in place.
- All information held on congregational rolls and gift aid lists etc. should not be revealed to third parties.
- Consent to use, storage and processing of information should be obtained from all data subjects (see under consent below).

Rights of data subjects

Data subjects can access most personal data held about them (some exemptions apply). It is important that all timescales are adhered to if a subject access request is made.

An individual can also serve a 'data subject notice' requiring the data controller to cease processing on the ground that the data is causing or is likely to cause unwarranted substantial damage or substantial distress to them. Similarly, a notice can be served to stop the use of data for the purposes of direct marketing. There is also a right to claim compensation for distress caused.

The Law Department can assist with any such correspondence recieved.

Manual Records

The Act has a definition of data so as to include some information held in manual (as opposed to electronic) format, namely data which is recorded as part of a 'relevant filing system'. This is defined as being any set of information relating to individuals to the extent that, although it is not processed electronically, the set is structured either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. A card index system or filing system of information about individuals arranged in alphabetical order following the persons' names would therefore be covered. However, a set of minutes of a meeting or other such documentation which might contain personal data would not fall within the definition if they were indexed by reference to date or subject matter and not by the names of the individuals concerned.

Obtaining Consent

If Sensitive Personal Data is involved – and information held on church databases will generally fall into this category - explicit consent must be obtained for that information to be stored and processed, particularly if there is any likelihood of the data being communicated in the future to a third party.

This would include the publishing of names, addresses and other information in a church magazine or on a church website and would also include the giving out of lists or labels to non-Church of Scotland bodies printed from databases containing the names and addresses of office-bearers and the like.

Explicit means that the consent of the data subject should be absolutely clear – e.g. the signing of an appropriate form or the ticking of a box on an electronic form. Where appropriate, the consent form should contain specific details of the purposes of the processing and as to the disclosures which may be made of the data to third

parties. Information should be held for no longer than is necessary. Examples of suggested consent forms are attached. These can be adapted to suit the needs of your congregation. Once a consent form has been signed it should be stored. Consent should also be revisited periodically, and particularly if the required use of the information is to change.

There have been a number of queries relating to obtaining consent from someone who has dementia. Whilst each case will depend on the extent of the dementia and the capacity of the individual concerned, under Scots Law, no one can provide consent on another's behalf unless there is a power of attorney (specific legal document) in place or the relatives of the person concerned have received authority to act on that person's behalf by court order. Unless however you anticipate particular difficulties arising, it should be in order to obtain consent from the person's next of kin/close relative who is responsible for organising their care - without requiring them to produce a power of attorney etc.

Internet Use

Personal data placed on the Internet is available for viewing world-wide, including countries where the use of personal data is not protected by legislation. Because of this it is always advisable and will often be essential to obtain explicit consent from individuals before publishing their personal data on a church web-site. However, given the use which may be made of the information, it may be better to adopt a policy of limiting what is published.

If information on individuals is being collected via a website, the page concerned should be set up to make it absolutely clear as to the identity of the body collecting the information, what personal data is being collected, processed and stored and for what purpose. This advice should be given before the site visitor is asked to provide the information, for example via an on-line application form. It is good practice to ask them to tick a box to confirm they are giving their consent to the collection of the data. If 'cookies' or other software is being used to collect information about visitors, this should be clearly stated. The Information Commissioner has indicated firmly that no personal data should be collected or retained unless it is strictly necessary for the organisation's purposes and that a practice should be made to delete regularly data which is out of date or no longer required – a principle which of course applies no matter how the data is originally obtained.

CCTV Cameras

Data Protection legislation covers the processing of images of individuals 'caught' on CCTV cameras which must accordingly be processed in accordance with the Data Protection Principles. If any congregation has such cameras in operation, this will trigger the requirement for the Presbytery of the bounds to notify. The Information Commissioner has published a Code of Practice regarding CCTV which can be downloaded from their website.

Further information

The Data Protection section of the Information Commissioner's website contains a wealth of information, together with a link to a training film which it is suggested could be used as a training mechanism for congregational office bearers and others handling and processing information:

http://www.ico.gov.uk/for_organisations/data_protection.aspx

The Law Department also welcomes any queries.

Summary

In short, Data Protection is everyone's responsibility and we would ask that all data is assessed with the following questions:

Is the Information:

- Needed?
- Accurate?
- Suitable?
- Secure?

Depending on the outcome of the above questions, appropriate action should be taken.