Data Protection Policy
Edinburgh Currie Kirk (Church of Scotland)
Registered Scottish Charity SC001554

1. Introduction

The Data Protection Act 1998 (the "Act") regulates the way in which information about living individuals (referred to as 'Data Subjects') is collected, stored or transferred. Compliance with the Act is important, because a failure to adhere its terms will potentially expose Currie Kirk *(the "*Congregation*")* or indeed in exceptional circumstances, office bearers as charity trustees and employees to complaints, large fines and/or bad publicity. It will also impact upon the Presbytery which has the role technically of being the "data controller" as defined in the Act for the congregation.

This policy therefore sets out what office bearers and employees must do when any personal data belonging to or provided by "Data Subjects", is collected, stored or transmitted onwards, or disposed of; it also seeks to provide general guidance in what is a very technical area of the law.

The Kirk Session requires all its trustees, office bearers and employees to comply with the Act and this policy (both as may be amended from time to time) when handling any Personal Data. A serious or persistent failure to do so may make trustees and office bearers liable to prosecution under the Act and employees liable to disciplinary action. If appropriate for their responsibilities, Trustees, office bearers and employees must make themselves familiar with the Act and take training on Data Protection issues.

The Kirk Session, following the recommendation of the Church of Scotland, has decided to appoint a Data Protection Officer who can acquire expertise in this area. He/she will liaise with the Presbytery Clerk as and when required and annually in advance of renewal of the Presbytery's registration with the Information Commissioner. The Data Protection Officer should be "visible" within the congregation as the person to whom queries in relation to compliance with the Act can be directed in the first instance. He/she should also report any issues or concerns to the Kirk Session and Presbytery and - ideally – be able to deliver training if necessary.

Any office bearer or employee who considers that this policy has not been followed in any instance should first contact the Data Protection Officer.

2. Data Protection General Responsibilities

Notification to the Information Commissioner

It is necessary to notify the Information Commissioner on an annual basis as to the Church bodies that are processing personal data. Although there are some exemptions, where data is being processed for pastoral reasons or where CCTV has been installed, notification is always required. This notification for the Congregation is made under the umbrella registration of the Presbytery of Edinburgh as the 'Data Controller'. This registration should cover all purposes for which data is processed by or on behalf of Currie Kirk.
The Presbytery's entry can be viewed at: www.ico.org.uk (Registration No. Z5659270)

The Data Protection Officer should be advised in writing of any plans to process data of classes or purposes not covered in the registered entry or of any amendments required to it as early as possible. Any doubts about whether any new processes are covered by the Registration should be discussed with the Data Protection Officer. He/she in turn will pass this information to the Presbytery Clerk if required. A failure to do so, or to knowingly process data other than in accordance with the registered entry, may constitute an offence under the Act.
The Data Protection Officer should keep a list of all copies of Personal Data which are held by Trustees, office bearers and employees and update the list regularly.
Extra copies of files of Personal Data should be restricted in general to those required for backup and the Data Protection Officer should be asked for approval before additional copies are made or transferred to others, whether Trustees, office bearers or employees.

Data Processing: The 8 Data Protection Principles

The Data Protection Act imposes a requirement to process Personal Data only in accordance with certain Principles. These require that all Personal Data must:

- Be processed fairly and lawfully;
- Be obtained for specific and lawful purposes;
- Be kept accurate and up to date;
- Be adequate, relevant and not excessive in relation to the purpose for which it is used;
- Not be kept for longer than is necessary for the purpose for which it is used;
- Be processed in accordance with the rights of Data Subjects;
- Be kept secure to prevent unauthorised processing and accidental loss, damage or destruction; and
- Not be transferred to any country outside the European Economic Area (EEA) (unless an exception applies).

Personal Data: Definition

Personal Data is data which relates to a living individual who can be identified from:
- that data; or
- from that data and other information which is in the possession of, or is likely to come into the possession of, the data user; and which
- is in electronic form or held manually in a relevant filing system.

This definition also includes any expression of opinion about the individual Data Subject and any indication of the intentions of the Data Controller or any other person in respect of the Data Subject.

Personal Data may either be held electronically or in paper records.

Sensitive Personal Data: Definition

Sensitive Personal Data is Personal Data about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, details of the commission or alleged commission of any offence and any court proceedings relating to the commission of an offence.

Sensitive Personal Data can only be processed under strict conditions including the express permission of the person concerned, unless a specific exemption applies. As a result, generally, if sensitive Personal Data is collected, appropriate steps will need to be taken to

ensure that explicit consent from the person concerned has been given to hold, use and retain this information.

A significant amount of Personal Data held by a Church of Scotland congregation will be Sensitive Personal Data as it could be indicative of a person's religious beliefs. Office bearers and employees are therefore urged to be extra vigilant when dealing with any Personal Data.

Transfer of Personal Data outside European Economic Area ("EEA")

The transfer of Personal Data to any country or location outside of the EEA is a breach of the Act unless:

- the data protection arrangements in the destination country have been approved by the EU Commission; or
- the recipient is a signatory to an EU approved data protection regime; or
- the recipient is bound by a contract that ensures that the data concerned will be adequately protected.

Given the links that the Church of Scotland maintains with other countries around the world, some Personal Data may fall into this category. Therefore, prior to transferring data outside the EEA or giving anyone outside the EEA access to personal data you must contact the Data Protection Officer, who will check the position with the Law Department of the Church of Scotland, if required.

Type of Personal Data

The type of data processed by the Congregation, its office bearers and employees is likely to fall into one of the following categories:

- Personal Data about office bearers, members, adherents, supporters and parishioners as Data Subjects; or
- Personal Data relating to employees as Data Subjects.

3. Personal Data about Members and Trustees

When an individual provides you with their contact details which you intend to record for future use you must hold, process and use that Data Subject's Personal Data in accordance with this policy and the 8 Data Protection Principles. In order to put the principles into practice you must also be aware of the type of information which is being collected, held or processed and therefore take into account the definitions of Personal Data and Sensitive Personal Data above.

Data must be obtained for a specific use and be kept accurate and up to date

People must be informed that we hold their Personal Data, why we hold it and what we will use it for. Where possible, when obtaining new contact information or other Personal Data or communicating with a contact for the first time, you should:

- Refer them to our Privacy Policy for information collected through the Currie Kirk web-site: A section of our web-site should be devoted to 'Our Privacy Policy'. This should follow appropriate parts of the Church of Scotland style which is available on the website: www.churchofscotland.org.uk/site_tools/privacy_policy.
- Otherwise, you should include a paragraph on any forms used for collecting Personal Data such as the following:

  "Currie Kirk is committed to protecting your privacy and safeguarding your personal data. We are registered with the Information Commissioner through the umbrella registration of the Presbytery of Edinburgh (Church of Scotland) and strive to comply fully with Data Protection law. We shall use the information you have provided for administration and communication of congregational matters and for appropriately processing and accounting for any donations in accordance with legal requirements. We will keep the data only for as long as necessary, and we will not use it for any other purpose without your prior consent. We will not disclose this information to any third party except as permitted or required by law. By providing this data we assume that you consent to its use in this way."

- On receipt of new or changed information you should check to see if your database already holds that person's details and is up to date and then as appropriate arrange for the details to be recorded/updated.
- If the use of the data is not going to be covered by the Privacy Policy, you must explain to the Data Subject what the use will be. If in doubt about the use of the Personal Data please discuss the matter with the Data Protection Officer who may check the position with the Church of Scotland Law Department, if required.
- Trustees, Office bearers and others whose names and contact details etc will be published on clipboard, accounts or the website should give their consent in writing for their data being used for this purpose and this should be renewed annually.
- Others who have given an email address for communications from the church will not have authorised the church to disclose it to others. Therefore, all emails to groups of people should use 'blind copy' so that all in the group do not see email addresses of all the others.

<u>Data must be held for no longer than necessary</u>

Employees and office bearers must monitor their own individual files of contacts (e.g. in Outlook and/or other databases) and update or remove details where appropriate. If you notice that the database is out of date, you should ensure that this is updated immediately. Any changes to basic contact details such as name, address, post code, email address, should be notified to the Roll Keeper who can then inform other data users.

If a Data Subject specifies that they do not wish you to use a particular form of contact with them or indeed that you are not to contact them at all, you must comply with this at once. You should ensure all databases/files are updated.

<u>Disclosures</u>

Personal Data must only be disclosed to those organisations and individuals who the Data Subject has consented may receive his or her data, or to organisations that have a legal right to receive the data without consent being given. Care must therefore be taken to ensure that Personal Data such as the names, addresses and telephone numbers of members are not disclosed either over the phone or in writing to non-Church personnel, without such consent being in place. Care should be taken when exhibiting records to Data

Subjects so that only the entry relating to the person concerned is exhibited to him/her and not also those of others who may still be alive.

Information Security

At minimum:

- 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. Ideally the office bearer or employee concerned should personally deliver the item by hand. 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 but not necessarily 'encryption'.
- Personal data must not be transmitted to, or held on, an office bearer's home computer, laptop or ipad without appropriate assurances from him/her that the foregoing safeguards will be put in place.
- Laptops, computers or memory sticks must have all personal data erased before disposal. Printouts or paper files containing Personal Data should be shredded before disposal.

Action to be taken if data goes missing or may have been copied illicitly

The Data Protection Officer must be informed immediately if any Personal Data goes missing or if you suspect that it may have been copied by an unauthorised person. An immediate investigation will be launched by the Kirk Session and the Presbytery Clerk will be informed. Depending on the circumstances, consideration will be given to making a report to the Information Commissioner.

Negligent transfer of data

If an office bearer or employee is negligent in transferring sensitive and confidential personal data this is conduct which may result in disciplinary action having to be taken and indeed in the case of an employee could be considered to be gross misconduct, which could result in summary dismissal. This is particularly likely to be the outcome if:

- The employee did not encrypt or password protect the data;
- The employee transferred the data in manual form without using secure means to do so or

- The employee transferred the data without seeking the appropriate approvals

Subject Access

Upon receipt of a written request from a data subject to see any personal data held which relates to them, contact should be made immediately with the Data Protection Officer who will contact the Presbytery Clerk to make arrangements for a response to be made within the statutory 40 day deadline.

4. Personal Data about Employees

Good employment practice dictates that, the Kirk Session as an employer, will need to keep information for purposes connected with an employee's employment during employment and for as long a period as is necessary following the termination of that employment.

The data recorded may include:

- information gathered about an employee and any references obtained during recruitment;
- details of terms of employment;
- salary and payroll information, tax, National Insurance information and pension details;
- appraisal information and performance management;
- details of grade and job duties and promotion/career development;
- health records;
- absence records, including holiday records and self-certification forms;
- details of any disciplinary investigations, warnings and proceedings and grievances;
- training and development records;
- contact names and addresses and next of kin information;
- all core and flexible benefits;
- correspondence with the Church as Employer and other information provided to the Employer.

The Kirk Session values the privacy of its staff and is aware of the responsibilities under the Act. The Kirk Session shall therefore process any personal information relating to staff fairly and lawfully and shall endeavour to comply with the Information Commissioner's code of practice on the use of Personal Data in employer/employee relationships.

The information held will be for the Kirk Session's management and administrative use only, but from time to time, the Kirk Session may need to disclose some information held about employees to relevant third parties or to another Organisation, solely for purposes connected with an employee's career or the management of the organisation.

Any Personal Data which is recorded or used in any way whether it is held on paper, computer or other media will have appropriate safeguards applied to it to ensure that it is in compliance with the Act.

The Kirk Session will make every effort to ensure that the information held is accurate and kept up to date but it is the responsibility of each individual employee to notify any changes. In the absence of evidence to the contrary, it will be assumed that the information is up to date.

5. Further information

Office bearers and employees who wish further information about data protection should look at the circular on the Church of Scotland website:
http://www.churchofscotland.org.uk/__data/assets/pdf_file/0003/2838/law_data_protection.pdf

Specific queries should be raised with the Data Protection Officer who, if appropriate, will take advice from the Law Department.

6. Review

The Kirk Session will review this policy on an on-going basis to ensure its continuing relevance and effectiveness in the light of any legislative or other developments. Any substantive changes will only be introduced after appropriate intimation has been given to all concerned.