STOW: ST MARY OF WEDALE AND HERIOT CHURCH OF SCOTLAND
CHARITY NO. SCO00228

DATA PROTECTION POLICY

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 Stow: St Mary of Wedale and Heriot Church (the "Congregation") or indeed in exceptional circumstances, office bearers as charity trustees, 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" for the congregation.

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

The Congregational Board requires all its office bearers 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 be regarded as misconduct and may be dealt with under the Discipline of Elders, Readers, Office Bearers Act 2010. If asked to do so, office bearers must therefore attend training on Data Protection issues. Any office bearer who considers that this policy has not been followed in any instance should contact the Clerk to the Congregational Board.

2. Data Protection General Responsibilities

Notification to the Information Commissioner

It is necessary to notify the Information Commissioner on an annual basis of the Church bodies that are processing personal data. Where data is being processed for pastoral reasons, notification is required. This notification for the Congregation is made under the umbrella registration of Melrose and Peebles Presbytery as the "Data Controller". The Presbytery's entry can be viewed at: www.ico.org.uk.

The Clerk to the Congregational Board 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. He/she in turn will pass this information to the Presbytery Clerk. 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.

Data Processing: The 8 Data Protection Principles

The Data Protection Act imposes a requirement only to process personal data 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 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 controller; 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.

A significant amount of information held by a Church of Scotland congregation will be sensitive personal data as it is likely to be indicative of a person's religious beliefs. The Information Commissioner is likely to view a breach of the Act in relation to such data as a more serious contravention than a similar breach in relation to "non-sensitive" personal data.

In relation to the holding of sensitive personal data, it is particularly important to ensure that individuals are in agreement with the information held about them and know the reasons why it is held. In some cases it may be necessary to obtain express written consent, and in all cases individuals should be made aware of the Congregation's Privacy Policy.

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. Before transferring such information outside the EEA or giving anyone outside the EEA access to personal data you should contact the Clerk to the Congregational Board, who will check the position with the Presbytery Clerk and/or Law Department, if required.

Type of Personal Data

The type of data processed by the Congregation and its office bearers is likely to fall into the category of: personal data about office bearers, members and parishioners.

3. Personal Data about Members and Trustees

When an individual provides you with their contact details which it is intended be recorded for future use in connection with the work of the congregation, you must hold, process and use that person's details in accordance with this policy and the 8 Data Protection Principles. In order to put the principles into practice the office bearer concerned 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 you are holding the information, what is held, why it is held and how it will be used. Where possible, when obtaining new contact information or other personal data or communicating with a contact for the first time, the relevant office bearer should:

- Refer them to the Privacy Policy, which should be displayed on the Congregation's website and notice boards in Church.

- If this is not possible, the next communication to the data subject concerned should include a paragraph in relation to contact details. Suggested wording is set out at Appendix 1; and

- A check should be made to see if the Congregation's database already holds that person's details and, if so, whether these are up to date. As appropriate, the details should then be recorded/updated and the individual told that their details are recorded for the Congregation's use.

Data must be held for no longer than necessary

Office-bearers and members must monitor their own individual contacts (e.g. in Outlook and/or other databases) and update or remove details where appropriate. If the responsible party notices that the database is out of date, he/she should ensure that this is updated immediately.

If someone specifies that they do not wish a particular form of contact with them or indeed that there is to be no contact with them at all, then the instruction must be complied with at once and all databases updated.

Disclosures

Personal data must only be disclosed to those organisations and individuals who the individual has agreed 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 information such as 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 with records such as the Baptismal Register 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 a minimum:

- Electronic data must be protected by standard password procedures with the "computer lock" facility in place when office bearers are away from the desk/workstation where information is held;

- Anyone working on church matters should ensure that Personal Data is 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 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 should be used. The recipient must be asked to confirm safe receipt as soon as the data arrives, and the sender is responsible for following up the matter if the confirmation is not received.

- Laptops and USB drives should have appropriate security and "encryption";

- Personal data must not be transmitted to an office bearer's home computer without appropriate assurances from him/her that the foregoing safeguards will be put in place. Personal data should not be sent to a work email address.

Action to be taken if data goes missing

The Presbytery Clerk as Data Protection Compliance Officer must be informed immediately if any confidential or sensitive data goes missing.

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 Presbytery Clerk who will make arrangements for a response to be made within the statutory 40 day deadline.

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/resources/subjects/law_circulars#data_protection

Specific queries should be raised with the Session Clerk/Clerk to the Congregational Board who, if appropriate, will take advice from the Presbytery Clerk and/or Law Department.

6. Review

The Congregational Board 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.