Data Protection Policy
Wellington Church of Scotland, SC000289
April 2018

1. Introduction

The European Union General Data Protection Regulation (GDPR, https://www.eugdpr.org/) regulates the way in which information about living individuals (referred to as 'data subjects') is collected, stored or transferred. Compliance with the GDPR is important, because a failure to adhere its terms will potentially expose *Wellington Church of Scotland, SC000289* 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 who have the role technically of being the "data controller" 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; it also seeks to provide general guidance in what is a very technical area of the law.

The Kirk Session requires all its office bearers and employees to comply with the GDPR 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 in accordance with the GPDR in the case of office bearers and in terms of the disciplinary policy applicable to them in the case of employees. If asked to do so, office bearers and employees must therefore attend training on Data Protection issues.

Any office bearer or employee who considers that this policy has not been followed in any instance should contact the Session Clerk of the Congregation.

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. 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 Presbytery of Glasgow as the 'Data Controller'. The Presbytery's entry can be viewed at: www.ico.org.uk

The Session Clerk 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 GDPR.

Data Processing: Data Protection Principles

The GDPR 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 (i.e. individuals have to be informed how their data is used);
- Be obtained for specific and lawful purposes (purpose limitation);
- 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
- The data processor and controller need to be able to demonstrate compliance with the principles set out

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.

Special Category Personal Data: Definition

Special category 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.

Special category data can only be processed under strict conditions.
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. Office bearers and employees are therefore urged to be extra vigilant when dealing with any such information, as the Information Commissioner is likely to view a breach of the GDPR in relation to such data as a more serious contravention than a similar breach in relation to "non-sensitive" personal data.

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 and parishioners; or
- personal data relating to employees.

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 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: https://wellingtonchurch.co.uk/privacy-policy/
- If the inquiry relates to participating in church activities, inform them about the Church's Data Protection Privacy Notice and ask them to sign our Data Protection Consent *pro forma*
- 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. If the use is not going to be for the purposes given in the Privacy Policy, the office bearer should explain what the use is likely to be. If in doubt about the use of the information this should be discussed with the Session Clerk who may check the position with the Law Department, if required.

Data must be held for no longer than necessary

Members, office-bearers, employees 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 this 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 or Marriage 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 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. 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. *Personal data should never 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. An immediate investigation will be launched by the Kirk Session. Depending on the circumstances, consideration should also be given to making a report to the Information Commissioner's Office (ICO) but before doing so guidance should be obtained from the Law Department.

Negligent transfer of data

If an office bearer or employee has been negligent in transferring sensitive and confidential personal data this will be 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 store in an encrypted format), compress and 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

In compliance with the accountability principle, any data breach (loss of data or negligent transfer) needs to be recorded, regardless of if it is deemed necessary to report it to the ICO.

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 30 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 GDPR. 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 GDPR.

The Kirk Session should make every effort to ensure that the information held is accurate and kept up to date but ultimately 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/resources/subjects/law_circulars#data_protection

Specific queries should be raised with the Session Clerk 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.