St Michael and All Angels' Church, Helensburgh

CHARITY Registered in Scotland SC006468

DATA PROTECTION POLICY

1. **Introduction**

The General Data Protection Regulations (EU) 2016/679) (GDPR) regulate the way in which information about living individuals is collected, stored or transferred. Compliance with the Regulations is important, because a failure to comply with the regulations potentially exposes St Michael and All Angels' Episcopal Church, Helensburgh, or indeed in exceptional circumstances, office bearers as charity trustees and employees to complaints, large fines and/or bad publicity.

GDPR for St Michaels is administered by a nominated person who is accountable to the Vestry Secretary as Data Protection Compliance Officer. Others may be temporarily assigned for specific purposes from time to time (for example to arrange a circulation or update data). This policy sets out what office bearers and employees must do when any individuals personal data is collected or stored; it also seeks to provide general guidance.

The Vestry requires all its office bearers and employees to comply with the Regulations 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 Act 1, 2010.

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

2. **Data Protection General Responsibilities**

Notification to the Information Commissioner:

St Michael and All Angels Church, are a not-for-profit organisation, and therefore relies on a a specific exemption from registration for bodies or associations that are not established or conducted for profit. The exemption applies because:

We only process data for the purposes of establishing or maintaining membership or support for St Michaels or administering activities for individuals who are members or have regular contact with St Michaels, and only hold information about individuals whose data we need to process for this exempt purpose. The personal data is restricted to personal information that is necessary for this exempt purpose

Under these conditions at the present time a data protection fee is not due to the ICO.

3. Data Processing: Principles and rules

The GDPR imposes a requirement to process Personal Data only on the following legal bases

(i) having the consent of the individual, or

(ii) processing in compliance with a legal obligation, or

(iii) processing for the legitimate interests of running the Vestry. 'Legitimate Interest' personal data may be processed if

(i) there is a genuine and legitimate reason for doing so; and

(ii) there is no harm to any of the Data Subject's rights and interests.

In practice almost ALL the personal data collected by St Michaels will be processed on this basis. Exceptions are discussed below under the heading Sensitive Personal Data.

4. **Personal Data: Definition**

Personal Data is data which is in electronic form or held manually in a relevant filing system, and which relates to a living individual who can be identified from:

That data itself; 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. This definition also includes any expression of opinion about an individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.

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 and prior consent of the person concerned, unless a specific exemption applies. As a result, if sensitive Personal Data is collected, appropriate steps will be taken to ensure that explicit consent from the person concerned has been given to hold, use and retain this information.

5. The rights of individuals

The GDPR provides the following rights for individuals

The right to be informed

When collecting personal data, individuals must be given certain information, such as your identity and how the intended to use their information. This is usually done through a privacy/data protection notice. For instance, the lawful basis for the processing of their data must be explained; the data retention periods (how long it is kept for); and that individuals have a right to complain to the ICO if they think that there is a problem in the way that you deal with their personal data.

The right to access (includes subject access requests)

Individuals have the right to be given confirmation that their data is being processed; and access to their personal data and supplementary information, (i.e. information that is usually supplied in a privacy notice).

Access Requests

The GDPR allows individuals to access their personal data so that they are aware of and can check the lawfulness of the use and the accuracy of the data.

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 Controller who will make arrangements for a response to be made within the statutory deadline. There will be a one month period from the receipt of such a request in which to comply.

If a request is refused the individual must be told why and that he/she has the right to complain to the ICO or a judicial remedy. There are limited circumstances where information may be withheld from the individual making the request, for example, if this would disclose personal data about a third party. If a subject access request is received and there is doubt as to how to respond, advice should be taken from the Diocese Registrar.

The right to rectification (correction)

Individuals have the right to have their personal data corrected (rectified) if it is inaccurate or incomplete. If the data has already been given to third parties, they must be told of the correction. Individuals must be advised of all third parties to whom the data has been given.

The right to erasure (also known as the right to be forgotten) Individuals have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Disclosures:

Every effort must 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 specific 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.

6. Protection Mechanisms

- Electronic data is to 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 will be positioned so that they are not visible to casual observers.
- Laptops and USB drives should have appropriate security and 'encryption'.
- 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 delivery 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 delivery service if there is any delay in the receipt of the data.
- Personal data transmitted to an office bearer's or data holders personal computer is permitted only where the Data Controller has recorded the location and that the foregoing safeguards are in place in advance of the transmission.
- NO identification of other addresses on a distribution list of electronic communications from any email is permitted. All electronic distribution lists should be addressed “bcc” (blind carbon copy).
- Personal data stored in manual form e.g. in files are 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 manual files and databases should be kept up to date and should have an archiving policy. Data no longer required must be regularly purged.
- Action to be taken if data goes missing

  The Vestry Secretary 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 Vestry. Depending on the circumstances, consideration will also be given to making a report to the Information Commissioner.

- 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.

7. **Personal Data about Employees**

Good employment practice dictates that, the Vestry 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 Vestry as Employer and other information provided to the Employer.

The Vestry values the privacy of its staff and is aware of its responsibilities under GDPR. The Vestry 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 Vestry management and administrative use only, but from time to time, the Vestry 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 compliant with the GDPR.

The Vestry 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 the Rector and/or Treasurer of any changes. In the absence of evidence to the contrary, it will be assumed that the information is up to date.

8. **Review**

The Vestry 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.

Appendix 1

Privacy Policy

This Privacy Policy covers the way in which the Vestry of St Michael and All Angels will use and disclose personal information that members, employees, volunteers, donors and other associates may provide us with.

Personal information includes any information that identifies you personally, such as your name, address, email address or telephone number.

The Vestry recognises the importance of your privacy and personal information and we have therefore outlined below how the Vestry collects, uses, discloses, and protects this information. We are registered with the Information Commissioner through the umbrella registration of St Michael and All Angels' Scottish Episcopal Church, Helensburgh and strive to comply fully with data protection law.

How We Collect Information

The Vestry receives and stores personal information provided by members, employees, volunteers and donors. This information can be supplied to us:

in writing or via email, by telephone conversation or on our website (e.g. when an individual becomes a member); or

by otherwise associating with the congregation or its organisations, (e.g. by enquiring about our work, activities, employment and volunteering opportunities); or

when donating money to the congregation or its organisations.

We may also receive information about you from third parties.

How We Use Information

We may use the information we collect:

in connection with membership records and for pastoral care purposes or in relation to your participation in our activities;

to communicate with you (e.g. by letter, email or telephone) for example to provide information relating to our work or new developments; to further our charitable aims, e.g. such as for fundraising activities;

for internal administration, such as for accounting purposes, or for analysing how we may better advance the Kingdom of God.

Disclosure of Information

The Vestry Secretary may need to disclose your information if required to do so by law.

Your Consent

For some purposes you will be asked to provide written explicit consent. By providing this consent you permit the use your personal data, including sensitive personal data such as on your health, to the collection and use of any information you provide in accordance with the above purposes and this privacy statement.

Storage and Security of Personal Information

The Vestry together with its office bearers and employees will use all reasonable endeavours to

ensure that personal information is held in a secure and confidential environment and when the information is no longer needed it will be placed in a secure archive, destroyed or permanently rendered anonymous.

You may request details of personal information which we hold about you . If you would like a copy of the information held on you, please contact Henry Douglass, the nominated controller who is accountable to the Data Protection Officer and Vestry of St Michael and All Angels Scottish Episcopal Church, Helensburgh. Our Data Protection Officer is Nicholas Davies (Vsec).

If you believe that any information we are holding on you is incorrect or incomplete, please write to or email as soon as possible to the address below*. Any information found to be incorrect will be corrected as quickly as possible.

Henry Douglass
Clutharden,
I Upper Adelaide Street,
Helensburgh
G84 7HT
Email. datacontroller@stmichaelhelensburgh.org.uk