Grace Church Milton Keynes
DATA PROTECTION POLICY

Responsibility:
All staff and volunteer data controllers

Effective date:
25/05/2018
Review date:
25/04/2019

Introduction
Grace Church holds personal data about trustees, employees, volunteers, members and regular attenders for Grace Church charitable purposes. This policy sets out how we obtain, store, and protect personal data, and the rules governing the use of personal data to which Grace Church employees and members may have access. Grace Church seeks to apply the Data Protection principles of FAIR, TRANSPARENT, and LAWFUL.

Definitions

Charitable purposes
The registered objects (charitable purposes) of Grace Church are

1. To advance Christianity in Milton Keynes and elsewhere, by any means or medium that is or may become available, in accordance with the Statement of Doctrine set out in the schedule
2. to relieve people who are in need because of:
   (i) sickness or poor health
   (ii) age
   (iii) financial hardship
   (iv) or some other reason

   by any proper means as the trustees think fit and including (where appropriate but not by way of limitation) the provision of advice; the promotion of good practices to combat such conditions and the provision of resources to alleviate or prevent such need
3. To advance education both general and vocational for children or adults but always within the principles of the Christian faith.

Personal data
Personal data is information that relates to identifiable individuals, including current and former employees, trustees, members, and volunteers. Personal data we hold will include individuals' contact details, financial and pay details for staff, and financial details for trustees and others claiming expenses
.
We also hold both personal and financial information on members who give financially to Grace church using Gift Aid.

Regarding our work with children and young people our registration form will hold details of the school that they attend.

Sensitive personal data
We will only request information regarding health conditions and additional needs, relevant to our care for our children and young people. This is in line with safeguarding procedures.

We will not ask for personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition sexuality, criminal offences, or related proceedings, and will ensure any biometric and genetic data is treated as sensitive — any exception will be for

safeguarding or health and safety reasons, and will be strictly controlled in accordance with Data Protection and Safeguarding regulations.

Data Controller
Grace Church and any person holding personal data on behalf of Grace Church is a data controller.

Scope
This policy applies to all trustees, staff, church members, regular attenders, and all others serving ministries or teams and members of recognised groups.

Responsibility
The trustees of Grace Church have appointed Patricia Gibb as our Administrator with responsibility for the day-to-day implementation of this policy.

Responsibilities of the IT Manager (Tim Gannon)

- Ensure all systems, services, software and equipment meet security standards
- Checking and scanning security hardware and software regularly
- Monitoring third-party services, such as cloud services that the company is using

Fair and lawful processing
Personal data will be fairly and lawfully processed in accordance with individuals' rights. This means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

The processing of all data must be:
- Necessary to our charitable purposes
- In our legitimate interests and not unduly prejudice the individual's privacy

Our Privacy Notice sets out the purposes for which we hold personal data and provides that everyone has the right to access their personal data that we hold.

Transparency
Being transparent and providing accessible information to individuals about how we will use their personal data is important.

In the table below are examples of data collected, and how we collect that data:

What personal information is being collected	Name and address, phone and email contact details, date of birth,
Who is collecting it	Administration staff
How is it collected	Printed cards completed by hand and signed or online form submitted to church office
Why is it being collected	To undertake charitable purposes
How will it be used	To contact recipients by phone, text or email
With whom will it be shared	Leaders, individual members, and attenders
Retention period	As long as being used and up to one year after

Sensitive personal data
In most cases where we process sensitive personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal

obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed, and to whom it will be disclosed.

Accuracy and relevance
Grace Church will endeavour to ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this. Individuals are entitled to ask that we correct inaccurate personal data relating to them.

Ownership of personal data
It is the responsibility of individuals to inform the Data Protection Officer if personal circumstances change, so that records are accurate and up to date.

Data security
Personal data must be kept secure against loss or misuse.

Storing data securely
- When data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords
- Data stored on CDs or memory sticks must be locked away when not being used
- The Data Protection Officer or IT Manager, must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location
- Data should be regularly backed up
- Data should never be saved directly to mobile devices
- All servers containing sensitive data must be approved and protected by security

Data retention
Personal data must not be kept any longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be consistent with data retention guidelines.

Training
All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Conditions for processing
We will ensure the use of personal data is justified using at least one of the documented conditions for processing. All staff who are responsible for processing personal data will be aware of the conditions for processing, and the conditions for processing will be available in the form of a Privacy Notice.

Transparency of data protection
Our Privacy Notice will be clearly displayed on the website, a copy will be given to anyone who requests it and will be made available to all who provide personal data.

Personal data
We will process personal data in compliance with data protection principles, and we will document the additional justification for the processing of any sensitive data.

Consent
The data that we collect is subject to active consent by the data subject (the data provider). This consent can be revoked at any time.

Criminal record checks
Disclosure and Debarring Service (DBS) criminal record checks are justified by law. DBS checks cannot be undertaken based solely on the consent of the subject.

Data portability
Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done free of any charge.

Right to be forgotten
A data subject may request that any information held on them is deleted or removed, and any third parties who process or uses that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default
Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The IT Manager will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

Transferring data internationally
There are restrictions on international transfers such that Personal Data must not be transferred anywhere outside the UK without consulting the Chair of trustees.

Data audit and register
Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches
All members of staff have an obligation to report actual or potential data protection compliance failures to enable the Data Controllers to:
- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Information Commissioner's Office of any compliance failures that are material either in their own right or as part of a pattern of failures

Monitoring
All staff and volunteers must observe this policy. The Trustees have overall responsibility and will monitor regularly to ensure compliance.

Consequences of failing to comply
The importance of this policy means that failure to comply with any requirement by a member of staff may lead to disciplinary action under our procedures.

Questions or concerns about anything in this policy should be directed to James Davies (Chair of Trustees).