St Mark's Church
LEAMINGTON SPA

DATA SECURITY POLICY

INDEX

Reviewed – September 2023

Review cycle – 3 years

Rugby Road, Leamington Spa, CV32 6DL
01926 421 004
www.st-marks.net

Reg. charity no. 1128485

Information Security

St Marks Church holds different types of information about members of the congregation, staff and other associated people:

Confidential information

GDPR-defined Special Categories of personal data (racial/ethnic origin, political opinion, religious beliefs, trade union membership, physical/mental health condition, sexual life, criminal record). This includes Safeguarding information, DBS checks, pastoral care records, children's work records, passwords

Restricted Information

GDPR-defined Personal Data (information that identifies living individuals including home / work address, age, telephone number, schools attended, photographs); some PCC / standing committee records. This includes Electoral roll details, FIRS attendees records

Information for Internal use only

Rotas, staff records, data consent forms, church booking forms, some financial records.

Publicly available information

Baptism, Wedding and Banns registers, some PCC records, Annual reports and accounts.

This information is kept in a variety of places, both physical and electronic. The security measures in place for these are:

Physical locations:

- Church office is locked and alarmed;
- Office filing cabinet is locked;
- The safe is in the Vicar's vestry;
- Upper Room is kept locked;
- Upper Room filing cabinet;
- Committee Room cupboard;

Electronic locations:

- Office PC is password protected
- Wifi is password protected
- Microsoft PCC Sharepoint site is password protected
- Emails are encrypted and only sent to and from the specific people involved in the processing of that information.
- Only email providers who comply with data protection measures are used, including, but not limited to: Google, Tiscali, BT, AOL.
- IT security is regularly reviewed and our systems updated as necessary to ensure that the evolving threat of cyber security is mitigated.

A list of those with access is held by the office.

Data Retention

The Church of England sets out how long various records should be kept for in their publication Keep or Bin – The Care of Church Records. and the relevant guidelines are summarised below:

- Baptism, Confirmation, Banns & Marriage registers – Kept indefinitely.
- Application forms related to the above - 2 years
- Contracts, tenders for works – 6 years
- Hall/ Church booking forms – 6 years
- Correspondence concerning appointments of ministers – 5 years
- Ministers' correspondence – current year + 3 years
- Electoral Roll – last complete review + 6 years
- Gift Aid Declarations – as long as they are valid + 6 years
- Clear DBS certificate or disclosure letter of confirmation – max 6 months after recruitment decision. Register of those cleared will be kept for 50 years.
- Risk assessment and management plan in event of unclear/ blemished DBS disclosure 50 years after employment ceases
- Records of safeguarding incidents/ risk assessments/ monitoring agreements – 50 years after the conclusion of the matter
- Personnel records of lay employees not working with children and vulnerable adults – 6 years after employment ceases
- Personnel records with contact with children and vulnerable adults including all documentation concerning any allegation and investigation regardless of the findings - Records of safeguarding incidents/ risk assessments/ monitoring agreements – 50 years after the conclusion of the matter
- Rota lists – current year + 2 years
- Membership Lists – last action + 5 years. This includes the following groups: FIRS, Toddlers, Children's Sunday Groups, Creche, Small Groups, Youth Group.
- Routine correspondence - current year + 3 years/ 6 years

Other items:

- Consent forms and spreadsheet generated from that information -5 years
- Yellow pages – yearly updates, old versions will be destroyed
- DBS list - updated yearly
- Food hygiene & First aid certificates - updated yearly
- Pastoral care records – only kept while current

Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. For example, the loss or theft of computer, hacking, sending data to the incorrect recipient, loss or alteration of data without permission.

A simple guide to responding to a personal data breach is available form the ICO website: https://ico.org.uk/for-organisations/sme-web-hub/72-hours-how-to-respond-to-a-personal-data-breach/

In brief, the steps are:

1. Information and containment

Find out what happened and why, how many people might be affected and what actions have been taken. Attempt to contain the breach; recover the data if possible, ask for it to be deleted, remotely wipe tech, contact the office or a church warden.

2. Assess the risks

Assess the risk of harm to the affected people. Risk of harm is any potential harm or detriment it may cause to people, for example safeguarding issues, identity theft or significant distress.

3. Report to the ICO

if there is a significant risk of harm, the Information Commissioners Office needs to be notified within 72 hours. Report the breach on the website of the Information Commissioners Office: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

When reporting a breach, the General Data Protection Regulations say you must provide:

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If there is no need to report the breach to the ICO, make a note of the breach and the reason for not notifying them.

4. Advise individuals

If there is a medium to high risk of harm, the individuals involved also need to be informed as soon as possible – by phone or email. Give advice on how they can protect themselves; change passwords, look out for fraudulent activity etc.

When telling individuals, give:

- a description in clear and plain language of the nature of the personal data breach,
- a contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach;

- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

5. Reflect

As with any security incident, investigate whether the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.