ESSSENTIAL 3A/G1A
GENERAL DATA PROTECTION REGULATIONS (GDPR) POLICY

Guidance adopted by ……
Guidance adopted by Trustees ……
Effective from ……
Guidance to be reviewed ……

Data Protection Officer ……
Effective from: ……
Contact: dataprotectionofficer@millbrooknazarene.co.uk

Millbrook Church of the Nazarene

General Data Protection Regulation (GDPR) Policy and Procedures

1. Introduction

Millbrook Church of the Nazarene is committed to protecting all information that we handle about people we support and work with, and to respecting people's rights under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

We are committed to protecting personal data from being misused, getting into the wrong hands as a result of poor security or being shared carelessly, or being inaccurate, as we are aware that people can be upset or harmed if any of these things happen.

This policy sets out how we collect, use, store, and share personal data. It should be read in conjunction with our GDPR Permission Form, Data Retention Schedule, and supporting checklists.

Before you collect or handle any personal data as part of your work (paid or otherwise) for the church, it is important that you take the time to read this policy carefully and understand what is required of you, as well as the organisation's responsibilities when we process data.

Our commitment within this policy is to support and train members of our leadership team and ministry heads in how to collect, store, and manage personal data in compliance with GDPR requirements effectively and safely. This ensures that all information is handled responsibly, securely, and with respect for the privacy of our church members and community.

2. What is Personal Data?

Personal data relates to a living individual who can be identified from that data. This may include names, addresses, phone numbers, email addresses, or other information which identifies a person.

Special category data includes information such as religious beliefs, health details, and safeguarding records. Extra care will always be taken with this information.

3. Who Are We?

Millbrook Church of the Nazarene is the Data Controller. This means the Church decides how your personal data is processed and for what purposes.

Contact details:
Millbrook Church of the Nazarene
Address: Millbrook Community Centre, 59a Drumahoe Rd, Millbrook, Larne BT40 2PF
Email: info@millbrooknazarene.co.uk

Our Purposes for Using Your Personal Data

We use personal data for the following purposes:
- To enable the Church to provide ministry, community activities, and services.
- To administer membership records and pastoral care.
- To manage employees, workers, and volunteers.
- To maintain accounts and records (including processing Gift Aid).
- To comply with safeguarding requirements.
- To communicate news, events, activities, prayer requests, and fundraising opportunities (with consent).
- To coordinate rotas, small groups, and volunteer teams.
- To manage communication channels, including WhatsApp community groups.
- To gather information through online tools (e.g. Google Forms) for leadership use only.

5. Legal Basis for Processing

We process data under the following lawful bases:
- Consent – e.g. where individuals have signed the Permission Form to receive communications by email, WhatsApp, or other channels.
- Employment/Legal obligation – e.g. processing Gift Aid for HMRC, safeguarding reporting processing staff concerns or pension administration
- Legitimate interests – e.g. leadership administration, rota planning, volunteer coordination, event organisation
- Religious purposes exemption – processing data of members, former members, and regular attenders in line with the Church's religious aims and pastoral care.

4. Consent

The Church obtains consent through its Permission Form, where individuals can choose how they would like to be contacted (post, phone, email, WhatsApp, etc.).

Consent may be withdrawn at any time by contacting any member of the leadership or pastoral team.

5. Our Commitments Regarding Your Personal Data

The Church complies with its obligations by:
- Keeping personal data up to date.
- Storing and destroying it securely.
- Not collecting or retaining excessive amounts of data.
- Protecting personal data from loss, misuse, or unauthorised access.
- Ensuring appropriate technical and organisational measures are in place.

In particular, we will make sure that all personal data is:

- Processed lawfully, fairly, and transparently – we will always be clear about how we use your information.
- Used only for specified and legitimate purposes – data will not be used for purposes other than those agreed.
- Limited to what is necessary **–** we will only collect the data we genuinely need.
- Accurate and kept up to date – we will correct or update records when informed.
- Retained only as long as necessary – data will not be kept longer than required for the agreed purpose.
- Kept secure **–** appropriate technical and organisational measures will be used to protect data.
- Handled in line with individual rights – we will respect your rights to access, correct, restrict, or delete your data.

6. Our Procedures Regarding Your Personal Data

Collection of Data

- Use official GDPR Permission Forms for all members, attendees, volunteers, and employees.
- Only collect data **necessary for church activities**, pastoral care, or legal obligations.
- Clearly inform individuals **why the data is being collected** and **how it will be used**.

Storage of Data

- Electronic data must be stored on **password-protected devices or approved cloud services** (e.g., Google Drive restricted to leadership).
- Paper records must be kept in **locked cabinets** within church premises.
- Access is restricted to those with a **legitimate need**, reviewed **annually**.

Data Usage

- Use personal data **only for its intended purpose** (e.g., communications, rota planning, safeguarding).
- Do not share personal data via non-secure methods (e.g., personal email or unapproved messaging apps).
- When using WhatsApp groups or Google Forms, ensure **explicit consent is obtained**, and data is **retained only for the necessary period**.

Training and Support

- New leaders and ministry heads receive **GDPR induction training**.
- Refresher sessions are provided to ensure **ongoing compliance and awareness**.
- Guidance documents, checklists, and FAQs are made available to support **day-to-day data handling**.

-

Data Review and Retention

- All records are **reviewed regularly** against the Church's Data Retention Schedule.
- Outdated or unnecessary data is **securely deleted or shredded**.

Reporting and Incident Management

- Suspected data breaches must be **reported immediately** to the Data Protection officer, or Trustees if officer is not available
- Breach incidents are **documented and investigated**, with the ICO notified if required.

Continuous Improvement

- Feedback from leaders, ministry heads, and members is encouraged to **improve data procedures**.
- Policies and procedures are **reviewed annually** or when legislation changes.

7. Special Sections

7.1 WhatsApp Community Groups
- Membership is voluntary and requires explicit consent which is obtained once members accept the WhatsApp community terms via the requested pathways
- Participants are informed that their phone number, display name, profile pictures and posted messages will be visible to other group members.
- Participants are informed WhatsApp/Meta may process data as platform provider, of which the Church has no control over Meta's internal processing.
- Groups are for church-related communication only.
- Admins (appointed leaders) ensure appropriate use and remove members on request or when the terms of the WhatsApp community groups have been breached
- WhatsApp groups (except specifically permitted youth only group chats) are limited to over 18s.
- Any member may leave any WhatsApp Community Groups or withdraw consent at any time by contacting a member of the leadership team to request phone number removal from Church records
- Participants will be informed that any safeguarding concerns identified or raised within the WhatsApp Communities as reported by admins or members will be recorded and relevant information disclosed to statutory authorities as required by law
.

7.1.1 WhatsApp group definitions
- Open discussion groups: free for approved members to share and post messages
- Admin-only broadcast/restricted groups: posting limited to assigned members only. Non-approved members will not be able to reply in-group, however direct contact details may be used by admins to follow up as needed

7.1.2 WhatsApp retention and deletion
- Message history: normally deleted within 6 months unless required for safeguarding or legal reasons.
- Requests for deletion will be actioned within 30 days subject to legal or safeguarding exceptions.

7.2 Google Forms
- Used for sign-ups, surveys, or feedback.
- Responses are accessible only to the Church leadership team.
- Data collected is retained only as long as necessary for the stated purpose (e.g. until an event is complete).
- Each form will include a statement reminding participants how their data will be used.

8. Sharing Your Data

Your personal data will be treated as strictly confidential. It will only be shared with others in the Church where necessary for ministry purposes, or with third parties outside the Church if required by law or with explicit consent.

We will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about the possibility of the data being shared (in a privacy notice), unless legal exemptions apply to informing data subjects about the sharing. Only authorised and properly instructed [staff/Trustees] are allowed to share personal data.

9. Data Retention

The Church keeps data only as long as necessary, following the Data Retention Schedule included in our GDPR Forms pack (e.g. Gift Aid – 6 years; accident reports – 3 years; consent forms – while the individual is a member/attender).

10. Data Security

- All electronic records are password protected.
- Devices used for Church work are secured and, where possible, encrypted.
- Cloud services (Google Drive, email) are restricted to Church leadership.
- Access permissions are reviewed annually.

11. Dealing with Data Protection Breaches

If any staff, volunteers, or contractors believe that personal data has been lost, misused, or that this policy has not been followed, they must report it immediately to the data protection officer via e-mail at: dataprotectionofficer@millbrooknazarene.co.uk.

The Church will keep a record of all data protection incidents, even if they do not need to be reported to the ICO.

If a breach is likely to put people's rights or freedoms at risk, the Church will report it to the ICO within 72 hours of becoming aware of it.

Where a breach creates a high risk to individuals (for example, bank account details being lost, or sensitive information being sent to the wrong person), the Church will also inform those affected without unnecessary delay so they can take steps to protect themselves.

12. Your Rights

Under GDPR, you have the right to:

- Request a copy of your personal data held by the Church.
- Request corrections if inaccurate.
- Request deletion of data when no longer required.
- Withdraw consent at any time.
- Restrict or object to certain processing.
- Lodge a complaint with the Information Commissioner's Office (ICO).

13. Further Processing

If the Church wishes to use your personal data for a new purpose not covered by this Policy, we will issue a new Privacy Notice explaining the change and seek consent where required.

14. Review

This Policy will be formally reviewed on an regular basis by Trustees, and updated in the event of any substantial changes to our data processing operations or relevant legislation

APPENDIX A

Church Data Retention Schedule

This Data Retention Schedule outlines how long various types of records should be kept by the church, in accordance with UK GDPR, the Data Protection Act 2018, and relevant safeguarding and financial regulations.

Data Type / Record	Purpose of Data	Retention Period	Reason / Legal Basis	Action After Retention Period
Financial Records (invoices, receipts, bank statements)	Accounting, audit, HMRC compliance	6 years after end of financial year	Companies Act 2006; HMRC requirements	Securely delete or shred paper/digital copies
Gift Aid Declarations	Claiming tax relief	6 years after last donation	HMRC requirement	Securely delete or shred
Minutes of Church Meetings (e.g. PCC, Trustees, Elders)	Governance and record of decisions	Permanent (archive)	Historical and legal significance	Transfer to secure or denominational archive
General Meeting Agendas and Notes	Operational reference	3 years	Practical reference period	Delete or shred
Membership Records (active members)	Administration, pastoral care	As long as person is a member + 2 years	Legitimate interest; consent	Delete or anonymise inactive records
Former Member Records	Historical record, safeguarding reference	2 years after membership ends (basic contact info may be kept longer with consent)	Legitimate interest	Delete or anonymise
Contact Details for Regular Attendees (non-members)	Communication about events and notices	As long as consent remains valid	Consent	Delete upon withdrawal of consent
Under 18 Sign-up Forms (e.g. Kids Club, Sunday School)	Consent, emergency contact, safeguarding	1 year after event, or until child turns 18 + 7 years if any incident occurs	Safeguarding best practice	Delete securely after period expires
Access NI / DBS Checks	Safeguarding vetting	Up to 6 months after recruitment decision	Access NI / DBS Code of Practice	Delete; retain only record that check was completed (date, certificate no.)

Volunteer / Staff Application Forms	Recruitment and safeguarding	6 months after unsuccessful application; duration of service + 6 years for successful candidates	Employment / safeguarding	Delete or archive securely
Pastoral Care Notes	Support and wellbeing of members	As long as necessary for care purpose	Legitimate interest; confidentiality	Delete when no longer needed or at subject's request
Email Lists / Newsletter Subscriptions	Communication	Until consent withdrawn	Consent	Delete upon unsubscribe
Safeguarding Incident Reports	Protection of children/vulnerable adults	75 years or in line with denominational safeguarding policy	Safeguarding obligations	Archive securely; do not delete early
Health & Safety Accident Reports	Legal compliance	3 years (adults) / until child turns 21 (for minors)	H&S regulations	Delete securely
Event Registration Forms (short-term)	Managing attendees, consent	Up to 1 year after event	Consent	Delete securely

General Retention & Security Principles

• Retain data only as long as necessary for its purpose.
• Review all records regularly.
• Use encryption and passwords for digital data; cross-cut shredders for paper.

APPENDIX B

Conditions for processing special category data:

1. The data subject has given explicit consent to the processing of special category personal data for one or more specified purposes, except where UK law provides that such processing remains prohibited despite consent:

    • In the context of our church/charity, this includes consent for activities such as pastoral care, prayer requests, membership records, and other faith-related services. Where appropriate, we may also rely on exemptions for not-for-profit bodies under Article 9(2)(d) of the UK GDPR, provided that processing relates solely to members or former members, is not disclosed externally without consent, and is subject to appropriate safeguards.

2. The processing of special category personal data is necessary for fulfilling employment-related obligations and exercising specific rights of the data controller or data subject under UK employment,

social security, or pension law. Such processing is authorised by applicable legislation and is subject to appropriate safeguards to protect the fundamental rights and interests of the data subject. The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

3. The processing of special category personal data is carried out in the course of our legitimate activities as a not-for-profit religious organisation. This processing relates solely to members, former members, or individuals with regular contact in connection with our charitable and faith-based purposes. Personal data is not disclosed outside the organisation without the explicit consent of the data subject, and appropriate safeguards are in place to protect their rights and interests. The processing relates to personal data which are manifestly made public by the data subject;

4. The processing of special category personal data is permitted where necessary for the establishment, exercise, or defence of legal claims, or when required by courts acting in their judicial capacity. This includes responding to legal proceedings, safeguarding organisational rights, and complying with judicial orders.

5. The processing of special category personal data is permitted where necessary for reasons of substantial public interest, as authorised by UK law. Such processing is proportionate to the aim pursued, respects the essence of the right to data protection, and is subject to suitable and specific safeguards to protect the fundamental rights and interests of the data subject.

6. The processing of special category personal data is permitted where necessary for preventive or occupational medicine, assessment of working capacity, medical diagnosis, or the provision and management of health or social care services. Such processing is carried out under UK law or pursuant to a contract with a health professional, and is subject to appropriate safeguards to protect the rights and interests of the data subject.

7. Read these alongside the Data Protection Act 2018, which adds more specific conditions and safeguards:

- Schedule 1 Part 2 contains specific ‘substantial public interest’ conditions for Article 9(2)(g).