

Background

The main New York law referenced here is the New York SHIELD Act, which amended New York's breach notification law and added a reasonable safeguard requirement for private information. New York General Business Law § 899-aa requires notice when computerized private information of New York residents is breached, and § 899-bb requires persons or businesses that own or license computerized data containing private information of New York residents to develop, implement, and maintain reasonable administrative, technical, and physical safeguards.

PRIVACY NOTICE

For Power of Faith Ministries International Inc., [New York Branch]

Effective Date:

Last Updated:

1. Introduction

This Privacy Notice explains how Power of Faith International Inc., Bronx, ("the Church," "we," "our," or "us") collects, uses, stores, shares, protects, and disposes of personal information in connection with our church, ministry, outreach, administrative, digital, financial, pastoral, volunteer, children's, youth, and community activities in New York.

As a church and religious organization, we collect and use personal information to support worship, discipleship, pastoral care, children's and youth ministry, membership administration, volunteer coordination, events, camps, conferences, community outreach, donations, communications, safeguarding, legal compliance, and general church administration.

We are committed to handling personal information responsibly, respectfully, securely, and in a manner that reflects both our Christian values and applicable legal obligations. This Privacy Notice is intended to help members, visitors, donors, parents, guardians, volunteers, staff, ministry workers, online users, and community participants understand how their information may be handled.

This Privacy Notice is written specifically for the Church's New York operations and New York-related personal information. If the Church also operates in other states or countries, separate privacy notices or supplemental notices may apply.

2. Organization Responsible for Personal Information

The Church is responsible for determining why and how personal information is collected, used, stored, shared, and protected in connection with its ministry and administrative activities.

Organization: Power of Faith Ministries International Inc., Bronx

Address: [Insert New York Address]

Email: [Insert Privacy Contact Email]

Telephone: [Insert Telephone Number]

Privacy Contact / Responsible Officer: [Insert Name or Office]

Questions, concerns, requests, or complaints about this Privacy Notice or the Church's handling of personal information should be directed to the contact listed above.

3. Scope of This Privacy Notice

This Privacy Notice applies to personal information collected or used by the Church in connection with:

- * Worship services;
- * Membership and visitor records;
- * Pastoral care and prayer requests;
- * Children's ministry;
- * Youth ministry;
- * Sunday School and Bible study;
- * Camps, retreats, conferences, and events;
- * Volunteer service;
- * Leadership and ministry assignments;
- * Donations, tithes, offerings, pledges, sponsorships, and event payments;
- * Church communications;
- * Websites, mobile apps, online forms, livestreams, and digital platforms;
- * Staff, volunteer, and ministry worker administration;
- * Safeguarding, safety, and emergency planning;
- * Legal, insurance, accounting, and governance obligations.

This Privacy Notice does not replace any specific consent form, media release, child/youth registration form, volunteer agreement, employee notice, donor notice, or event-specific privacy statement that the Church may use.

Where a more specific notice or consent form applies, that document should be read together with this Privacy Notice.

4. Categories of Personal Information We May Collect

The Church may collect different types of personal information depending on your relationship with the Church and the activity involved.

4.1 Contact and Identification Information

We may collect:

- * Full name;
- * Mailing address;
- * Email address;
- * Telephone number;
- * Date of birth or age group;
- * Gender, where relevant to ministry participation, accommodation, or safeguarding;
- * Parent or guardian name and contact details;
- * Emergency contact information;
- * Family or household information voluntarily provided;
- * Membership, visitor, or ministry participant status.

4.2 Church Membership and Ministry Participation Information

We may collect information relating to:

- * Church membership;
- * Visitor records;
- * Baptism, dedication, confirmation, or other ministry records;
- * Attendance or participation in worship services, Bible studies, classes, events, camps, retreats, conferences, ministries, or programs;
- * Small group or discipleship group participation;
- * Ministry involvement;
- * Volunteer service;
- * Leadership roles;
- * Spiritual development programs;
- * Pastoral care follow-up;
- * Requests for prayer, visitation, benevolence, counseling, or spiritual support.

4.3 Children and Youth Information

For children and youth ministries, we may collect:

- * Child or youth name;
- * Date of birth or age;
- * Parent or guardian name and contact details;
- * Emergency contact details;
- * Medical, allergy, dietary, mobility, or accommodation information relevant to participation and safety;
- * School grade or age group;
- * Event, camp, retreat, or class registration details;
- * Transportation permissions;
- * Check-in and check-out information;
- * Media consent information;
- * Incident, safeguarding, or safety-related information, where necessary.

4.4 Donation, Giving, and Financial Information

We may collect information relating to:

- * Donations;
- * Tithes;
- * Offerings;
- * Pledges;
- * Sponsorships;
- * Event payments;
- * Registration fees;
- * Giving history;
- * Donor contact information;
- * Receipts and acknowledgments;
- * Limited payment transaction information;
- * Accounting and audit records.

Where online giving or card payments are used, payment information is generally processed through third-party payment processors. The Church should avoid storing full credit card or debit card numbers unless there is a lawful, necessary, and secure reason to do so.

4.5 Digital and Technical Information

When you use our website, mobile app, livestream, online forms, online giving tools, email links, or other digital platforms, we may collect:

- * IP address;
- * Device information;
- * Browser type;
- * Operating system;
- * Usage data;
- * App activity;
- * Registration form submissions;
- * Communication preferences;
- * Email engagement information;
- * Cookies, pixels, analytics data, or similar digital tracking data, where used.

4.6 Sensitive Personal Information

We may collect sensitive personal information only where appropriate, necessary, voluntarily provided, or required for safety, ministry, administrative, or legal purposes. This may include:

- * Health-related information provided for event, camp, travel, emergency, or accommodation purposes;
- * Medical allergies or medications relevant to participation and safety;
- * Emergency medical information;
- * Pastoral care information;
- * Prayer requests;
- * Counseling or spiritual care information;
- * Benevolence or hardship information;
- * Information about minors;
- * Background check information for certain volunteers, staff, or ministry workers;
- * Financial information connected with donations, assistance, or accounting;

* Religious affiliation, membership, participation, or spiritual care information.

Sensitive personal information will be handled with additional care and accessed only by authorized individuals with a legitimate ministry, administrative, safeguarding, legal, financial, or operational need to know.

5. Purposes for Which We Use Personal Information

The Church may use personal information for the following purposes.

5.1 Worship, Ministry, and Discipleship

We may use personal information to:

- * Support worship services and ministry programs;
- * Maintain membership and visitor records;
- * Provide pastoral care, prayer, discipleship, visitation, and spiritual support;
- * Organize Bible studies, Sunday School, small groups, and discipleship activities;
- * Coordinate ministry participation and leadership involvement;
- * Follow up with members, visitors, and participants.

5.2 Children's and Youth Ministry

We may use personal information to:

- * Register children and youth for ministry activities;
- * Communicate with parents and guardians;
- * Manage attendance, safety, and supervision;
- * Confirm parental or guardian permissions;
- * Plan age-appropriate programming;
- * Manage transportation and emergency arrangements;
- * Address medical, allergy, dietary, mobility, or accommodation needs;
- * Support safeguarding and child protection practices;
- * Document incidents or concerns where necessary.

5.3 Events, Camps, Conferences, Retreats, and Programs

We may use personal information to:

- * Register participants;
- * Process payments;
- * Communicate event information;
- * Manage attendance;
- * Coordinate meals, lodging, transportation, seating, security, and logistics;
- * Maintain emergency contact information;
- * Support health and safety planning;
- * Manage volunteer and staff assignments;
- * Provide certificates, confirmations, or follow-up communication.

5.4 Donations, Giving, and Financial Administration

We may use personal information to:

- * Process donations, tithes, offerings, pledges, and sponsorships;
- * Issue receipts and acknowledgments;
- * Maintain donor and accounting records;
- * Support financial reporting, stewardship, and audit processes;
- * Comply with applicable tax, accounting, legal, and nonprofit obligations;
- * Communicate with donors about giving opportunities, ministry needs, and campaigns.

5.5 Communications

We may use personal information to send:

- * Church announcements;
- * Ministry updates;
- * Event invitations;
- * Registration confirmations;
- * Devotionals;
- * Newsletters;
- * Prayer points;
- * Volunteer updates;
- * Giving or fundraising communications;
- * Safety notices;
- * Administrative messages;
- * App notifications;
- * Email, SMS, phone, or mail communications.

Individuals may opt out of certain non-essential communications. However, the Church may still send necessary administrative, transactional, safety, donation, event, or ministry-related messages.

5.6 Media, Photography, Video, Audio, and Livestreaming

We may use photographs, video, audio, livestream footage, testimonies, and event recordings to:

- * Share worship services;
- * Document church life;
- * Promote church events;
- * Report on ministry activities;
- * Encourage participation;
- * Maintain historical records;
- * Share testimonies;
- * Publish content on the Church's website, app, social media, printed materials, or other media platforms.

5.7 Safety, Security, and Safeguarding

We may use personal information to:

- * Protect children, youth, vulnerable adults, members, visitors, staff, volunteers, and the public;
- * Manage emergencies;
- * Document incidents;
- * Conduct appropriate volunteer or staff screening;
- * Respond to safeguarding concerns;

- * Prevent fraud, misuse, misconduct, unauthorized access, or harm;
- * Support insurance, legal, and risk-management processes.

5.8 Legal, Administrative, Governance, and Compliance Purposes

We may use personal information to:

- * Comply with applicable laws;
- * Maintain church governance records;
- * Manage nonprofit or administrative obligations;
- * Respond to lawful requests;
- * Maintain insurance and risk records;
- * Handle disputes, complaints, or legal claims;
- * Conduct audits or internal reviews;
- * Protect the Church's rights, property, ministry, and legal interests.

6. Legal, Operational, Ministry, and Consent-Based Reasons for Use

New York privacy and data security law does not use the same "lawful basis" structure found in some international privacy laws. However, the Church will seek to collect and use personal information only where there is a proper reason to do so.

Depending on the situation, we may collect and use personal information based on:

- * Your consent;
- * Parent or guardian consent for minors where appropriate or required;
- * The need to provide ministry services, pastoral care, events, programs, or communications;
- * The need to process donations, payments, registrations, or receipts;
- * The need to protect health, safety, security, or safeguarding interests;
- * Compliance with legal, tax, accounting, nonprofit, employment, or regulatory obligations;
- * The Church's legitimate ministry, administrative, governance, and operational interests;
- * The need to establish, exercise, or defend legal rights.

Where we rely on consent, you may withdraw consent where applicable. Withdrawal of consent may not affect information already used or retained for legal, safeguarding, accounting, insurance, pastoral, or administrative reasons.

7. New York-Specific Privacy and Data Security Considerations

The Church will seek to handle New York personal information in line with applicable New York privacy, security, breach notification, and data protection requirements.

7.1 New York SHIELD Act

New York's SHIELD Act requires certain persons or businesses that own or license computerized data containing private information of New York residents to maintain reasonable safeguards to protect the security, confidentiality, and integrity of that private information.

The Church should treat this requirement seriously where it owns, licenses, stores, or manages computerized private information of New York residents.

7.2 Reasonable Administrative Safeguards

The Church should maintain reasonable administrative safeguards appropriate to its size, resources, ministry activities, and the sensitivity of the information it handles.

Administrative safeguards may include:

- * Assigning responsibility for privacy and data security oversight;
- * Identifying reasonably foreseeable internal and external risks;
- * Assessing safeguards already in place;
- * Training pastors, staff, ministry leaders, and volunteers who handle personal information;
- * Selecting service providers capable of maintaining appropriate safeguards;
- * Requiring service providers to maintain reasonable safeguards by contract where possible;
- * Adjusting safeguards as ministry activities, systems, risks, or legal requirements change;
- * Limiting access to personal information to authorized persons with a legitimate need to know.

7.3 Reasonable Technical Safeguards

The Church should maintain reasonable technical safeguards appropriate to the nature of its systems and information.

Technical safeguards may include:

- * Assessing risks in network and software design;
- * Assessing risks in information processing, transmission, and storage;
- * Detecting, preventing, and responding to attacks or system failures;
- * Testing and monitoring the effectiveness of key controls;
- * Password protection;
- * Multi-factor authentication where appropriate;
- * Encryption where appropriate;
- * Secure cloud storage;
- * Access controls;
- * Regular review of user permissions;
- * Secure configuration of websites, apps, forms, email systems, giving platforms, and cloud drives.

7.4 Reasonable Physical Safeguards

The Church should maintain reasonable physical safeguards for records, devices, and locations where personal information is stored or accessed.

Physical safeguards may include:

- * Assessing risks of information storage and disposal;
- * Detecting, preventing, and responding to intrusions;
- * Protecting records against unauthorized access, use, or disclosure;
- * Locking file cabinets or rooms containing sensitive records;
- * Limiting access to offices or storage areas;
- * Securing laptops, tablets, phones, and portable drives;
- * Securely disposing of records after the applicable retention period;
- * Shredding paper records containing sensitive information;
- * Securely erasing electronic records when no longer needed.

7.5 Private Information Protected Under New York Breach Law

For breach notification and security purposes, New York law gives particular attention to computerized private information, including combinations of personal identifiers with certain sensitive data elements.

The Church should give special care to records involving:

- * Social Security numbers;
- * Driver's license numbers;
- * Non-driver identification card numbers;
- * Account numbers, credit card numbers, or debit card numbers with access codes, passwords, or security codes;
- * Biometric information;
- * Usernames or email addresses with passwords or security questions and answers that would permit access to an online account;
- * Medical information;
- * Health insurance information;
- * Other information treated as private information under applicable New York law.

7.6 New York Breach Notification

If the Church experiences a breach involving private information of New York residents, it should promptly assess whether notice is required to affected individuals and to appropriate New York authorities.

The Church should consult legal counsel, where appropriate, before determining whether notice is required, what notice must contain, and which authorities must be notified.

8. Privacy Choices and Requests

Depending on the nature of your relationship with the Church and applicable law, you may request that we:

- * Confirm whether we hold personal information about you;
- * Provide access to certain personal information;
- * Correct inaccurate or outdated information;
- * Update your contact details;
- * Update communication preferences;
- * Remove you from certain mailing lists;
- * Stop using your image or media in future publications, where reasonably possible;
- * Delete certain information, where it is no longer needed and where deletion is not restricted by legal, safeguarding, financial, insurance, pastoral, archival, or administrative reasons;
- * Restrict certain uses of your personal information, where appropriate.

The Church may need to verify your identity before fulfilling a request. Parents or guardians may be required to verify their authority before making requests relating to a minor.

The Church may deny or limit a request where necessary to:

- * Comply with the law;
- * Maintain donation, tax, accounting, or audit records;
- * Protect children, youth, vulnerable adults, or others;
- * Maintain safeguarding or incident records;
- * Complete a transaction or event registration;
- * Preserve church membership, pastoral, or ministry records;
- * Protect legal rights;
- * Prevent fraud or misuse;
- * Maintain records required for insurance, governance, or dispute resolution.

9. Sources of Personal Information

We may collect personal information from:

- * You directly;
- * Parents or guardians;
- * Family members, where appropriate;
- * Pastors, ministry leaders, staff, or volunteers;
- * Membership forms;
- * Visitor cards;
- * Event registration forms;
- * Children's and youth registration forms;
- * Online forms;
- * Donation and payment platforms;
- * Church websites, apps, and digital platforms;
- * Email, SMS, telephone, or social media communications;
- * Background check providers, where applicable;
- * Third-party service providers supporting church operations.

We will not intentionally collect personal information from third parties unless there is a legitimate ministry, administrative, safeguarding, legal, or operational reason to do so.

10. How Long We Keep Personal Information

The Church will keep personal information only as long as reasonably necessary for the purpose for which it was collected, unless a longer period is required or appropriate for legal, accounting, tax, safeguarding, insurance, pastoral, historical, archival, governance, or dispute-resolution purposes.

Examples include:

- * Donation and accounting records may be retained for tax, audit, and financial reporting purposes;
- * Children's and youth records may be retained for safeguarding, insurance, incident management, and legal purposes;
- * Membership and ministry records may be retained for pastoral, administrative, and historical purposes;
- * Volunteer and staff screening records may be retained for safeguarding, legal, and governance purposes;
- * Event records may be retained for administrative, safety, financial, or historical purposes;
- * Media consent records may be retained for as long as related media is used, published, archived, or reasonably needed.

When information is no longer needed, the Church will seek to securely delete, shred, erase, anonymize, archive, or otherwise dispose of the information in a manner appropriate to its sensitivity.

11. Secure Disposal of Personal Information

When personal information is no longer required, the Church will take reasonable steps to dispose of it securely.

Secure disposal may include:

- * Shredding paper records;
- * Securely deleting electronic files;
- * Erasing storage devices;
- * Limiting access to archived records;
- * Using reputable document destruction providers;
- * Removing unnecessary copies from shared drives, email accounts, or cloud systems;
- * Ensuring third-party providers securely dispose of information when no longer needed.

Special care should be taken when disposing of records containing financial information, donor records, children's or youth information, health-related information, pastoral care information, prayer requests, background check records, or identification information.

12. How We Protect Personal Information

The Church will use reasonable administrative, technical, and physical safeguards to protect personal information.

These safeguards may include:

- * Privacy and confidentiality expectations for pastors, staff, ministry leaders, and volunteers;
- * Limiting access based on role and need to know;
- * Password-protected systems;
- * Secure storage of paper files;
- * Secure cloud-based platforms where appropriate;
- * Encryption where appropriate;
- * Multi-factor authentication where appropriate;
- * Regular review of user access;
- * Caution when using shared devices or shared email accounts;
- * Secure handling of donor and payment information;
- * Vendor due diligence;
- * Incident response procedures;
- * Training for persons who handle sensitive information;
- * Safeguarding procedures for children and youth records;
- * Careful handling of pastoral care, prayer, benevolence, and counseling information.

No system is completely secure. However, the Church will take reasonable steps to protect personal information from unauthorized access, loss, misuse, disclosure, alteration, or destruction.

13. Sharing Personal Information

The Church may share personal information only where appropriate and necessary.

13.1 Internal Sharing

Personal information may be shared internally with pastors, staff, board members, ministry leaders, volunteers, or authorized personnel who need the information for ministry, administration, safeguarding, pastoral care, finance, events, communications, or legal compliance.

13.2 Service Providers

The Church may share personal information with trusted third-party service providers that help us operate. These may include:

- * Website providers;
- * Church app providers;
- * Online giving platforms;
- * Payment processors;
- * Event registration systems;
- * Email and SMS providers;
- * Accounting and bookkeeping providers;
- * Cloud storage providers;
- * IT support providers;
- * Background check providers;
- * Insurance providers;
- * Legal, audit, or compliance advisers;
- * Livestream and media platforms.

Service providers should be required to use personal information only for the services they provide to the Church and to protect the information appropriately.

13.3 Legal, Safety, and Safeguarding Disclosures

The Church may disclose personal information where necessary or appropriate to:

- * Comply with law;
- * Respond to lawful requests;
- * Protect children, youth, vulnerable adults, members, staff, volunteers, visitors, or the public;
- * Report abuse, neglect, threats, or safeguarding concerns;
- * Respond to emergencies;
- * Prevent fraud, unauthorized access, or misuse;
- * Protect church property, rights, ministry, or legal interests;
- * Establish, exercise, or defend legal claims;
- * Cooperate with law enforcement, regulatory authorities, insurers, or legal advisers.

13.4 No Sale of Personal Information

The Church does not sell member, visitor, donor, child, youth, pastoral care, prayer request, volunteer, or ministry participant information.

If the Church ever engages in digital advertising, analytics, data-sharing, or targeted advertising practices that may be treated as a “sale” or similar regulated activity under applicable law, the Church should update this Privacy Notice and provide any required choices.

14. International Transfers

If the Church uses cloud-based platforms, international service providers, overseas ministry partners, denominational offices, or affiliated churches outside the United States, personal information may be accessed from, transferred to, or stored in another country.

Where this occurs, the Church will seek to use reasonable safeguards appropriate to the nature of the information, the receiving party, and the purpose of the transfer.

Individuals should understand that privacy and data protection laws may differ from country to country.

15. Photography, Video, Audio, Live streaming, and Media

The Church may photograph, record, livestream, or otherwise capture images, video, audio, or testimonies during worship services, events, camps, conferences, retreats, outreach activities, and other ministry programs.

These materials may be used for:

- * Worship live streaming;
- * Church communication;
- * Ministry reporting;
- * Social media;
- * Website or app content;
- * Newsletters;
- * Promotional materials;
- * Historical records;
- * Testimonies;
- * Training or internal reporting.

The Church will seek appropriate consent where necessary or appropriate, especially for:

- * Children and youth;
- * Vulnerable individuals;
- * Private pastoral care settings;
- * Counseling or prayer ministry settings;
- * Sensitive testimonies;
- * Medical, benevolence, or safeguarding situations;
- * Any context where a person has a reasonable expectation of privacy.

Parents or guardians may be asked to provide media consent for minors. If you do not wish to be photographed, recorded, live-streamed, or published, you should notify the Church as early as possible.

The Church will make reasonable efforts to honor such requests, but may not be able to remove images, recordings, or livestream content that has already been published, archived, printed, shared, or distributed.

16. Children and Youth Privacy

The Church takes the privacy and safety of children and youth seriously.

For children's and youth programs, the Church will seek to collect only the information reasonably needed for ministry participation, communication, safety, safeguarding, emergency response, transportation, event planning, and administration.

The Church may seek parent or guardian consent for:

- * Registration;
- * Participation in children's or youth activities;
- * Camps, retreats, conferences, and offsite events;
- * Transportation;
- * Emergency medical information;
- * Photography, video, audio, livestreaming, or publication;
- * Online activities involving children;
- * Communication with minors;
- * Collection of sensitive information.

The Church will not knowingly publish sensitive personal information about a child or youth without appropriate authorization.

Where online services are directed to children under 13, or where the Church knowingly collects personal information online from children under 13, the Church should follow applicable children's online privacy requirements, including parental notice and verifiable parental consent where required.

17. Pastoral Care, Prayer Requests, and Counseling Information

The Church may receive personal, spiritual, family, health, financial, or sensitive information through:

- * Pastoral care;
- * Prayer requests;
- * Counseling or spiritual care;
- * Altar ministry;
- * Visitation;
- * Benevolence requests;
- * Deliverance ministry;
- * Discipleship;
- * Small groups;
- * Ministry conversations.

The Church will seek to treat such information with care, respect, and confidentiality.

However, confidentiality may be limited where disclosure is necessary or appropriate to:

- * Protect a person from harm;
- * Protect a child, youth, vulnerable adult, or the public;
- * Report abuse, neglect, threats, or safeguarding concerns;

- * Respond to emergencies;
- * Comply with the law;
- * Seek appropriate pastoral, legal, professional, or safeguarding guidance;
- * Protect the Church's legal interests.

Pastoral care and prayer ministry are not automatically the same as licensed medical, psychological, legal, or financial services. Where professional assistance is needed, the Church may encourage individuals to seek qualified professional support.

18. Cookies, Analytics, and Digital Tracking

The Church's website, app, email systems, livestream platforms, or digital tools may use cookies, pixels, analytics tools, or similar technologies to:

- * Operate digital services;
- * Improve website or app performance;
- * Understand engagement;
- * Manage registrations;
- * Support online giving;
- * Provide livestreams and media content;
- * Measure email engagement;
- * Improve communications and outreach.

Where required or appropriate, the Church will provide notice or choices about cookies and similar technologies.

You may be able to control cookies through your browser or device settings. Disabling cookies may affect how some websites, apps, or online features operate.

The Church should avoid using advertising pixels, retargeting tools, or other targeted advertising technologies that involve sensitive information related to church participation, donors, youth, pastoral care, or prayer unless appropriate legal review has been completed and privacy notices have been updated.

19. Email, SMS, Telephone, and App Communications

The Church may communicate by email, SMS, telephone, postal mail, app notification, or other channels.

Communications may include:

- * Worship service information;
- * Ministry updates;
- * Event invitations;
- * Registration confirmations;
- * Volunteer coordination;
- * Devotionals;
- * Prayer points;
- * Newsletters;
- * Fundraising or giving information;
- * Emergency or safety notices;
- * Administrative messages.

Individuals may opt out of certain non-essential communications. However, the Church may still send necessary administrative, transactional, event-related, donation-related, safety, or ministry-related messages.

For mass texting, automated calls, prerecorded messages, or promotional communications, the Church should obtain appropriate consent and provide opt-out instructions where required.

20. Donor Privacy

The Church respects the privacy of donors.

Donor information may be used to:

- * Process donations, tithes, offerings, pledges, and sponsorships;
- * Issue receipts and acknowledgments;
- * Maintain financial and accounting records;
- * Support tax, audit, and legal obligations;
- * Communicate about ministry needs, fundraising campaigns, or giving opportunities;
- * Provide internal financial reporting;
- * Support stewardship and accountability.

The Church does not sell donor lists.

Donor information should be accessed only by authorized persons who need it for financial, administrative, pastoral, governance, audit, legal, or ministry purposes.

21. Volunteer, Staff, and Ministry Worker Information

If you apply to serve, volunteer, work, teach, lead, drive, handle funds, provide pastoral care, work with children or youth, or serve in a sensitive ministry role, the Church may collect additional information, such as:

- * Application details;
- * References;
- * Background check information;
- * Training records;
- * Ministry assignments;
- * Availability;
- * Emergency contact information;
- * Conduct, performance, or disciplinary records where applicable;
- * Safeguarding or incident records where applicable.

This information may be used for:

- * Ministry placement;
- * Employment or volunteer administration;
- * Safeguarding;
- * Risk management;
- * Legal compliance;
- * Governance;
- * Training;

- * Accountability.

Access to this information should be limited to authorized individuals with a legitimate need to know.

22. Background Checks and Safeguarding Screening

The Church may conduct background checks or other screening for individuals who serve in sensitive roles, including roles involving:

- * Children;
- * Youth;
- * Vulnerable adults;
- * Transportation;
- * Counseling or pastoral care;
- * Financial handling;
- * Security;
- * Leadership;
- * Access to sensitive personal information.

Background check information will be handled confidentially and used only for appropriate ministry, employment, safeguarding, legal, or risk-management purposes.

The Church should use reputable background check providers and comply with applicable consent, notice, and employment-related requirements.

23. Data Breach and Security Incident Response

A data breach or security incident may occur when personal information is accessed, acquired, disclosed, altered, lost, or used without authorization.

If the Church becomes aware of a suspected or actual breach involving personal information, the Church will take appropriate steps to:

- * Investigate the incident;
- * Contain the incident;
- * Determine what information was involved;
- * Identify affected individuals where possible;
- * Assess legal notification obligations;
- * Notify affected individuals, regulators, law enforcement, service providers, insurers, or other parties where required or appropriate;
- * Document decisions and actions taken;
- * Review and improve safeguards where appropriate.

For New York residents, certain breaches involving private information may require notification to affected individuals in New York and appropriate New York authorities.

The Church should seek legal guidance when assessing New York breach notification obligations, including whether notice is required, the timing of notice, the content of notice, and which New York authorities must be notified.

If a third-party service provider experiences a breach involving personal information handled for the Church, the Church expects that provider to notify the Church promptly and provide the information needed for the Church to meet its legal obligations.

24. Third-Party Links and Platforms

The Church's website, app, emails, social media pages, livestreams, or digital communications may include links to third-party websites or platforms.

These may include:

- * Online giving platforms;
- * Payment processors;
- * Event registration tools;
- * Social media platforms;
- * Livestream platforms;
- * Video hosting platforms;
- * Bible or devotional tools;
- * External ministry partners;
- * Vendor websites.

The Church is not responsible for the privacy practices of third-party websites or platforms. Individuals should review the privacy notices of those third parties before providing personal information.

25. Governance and Accountability

The Church will seek to maintain reasonable privacy and data protection governance appropriate to its size, structure, ministry activities, and legal obligations.

This may include:

- * Assigning responsibility for privacy oversight;
- * Maintaining privacy and confidentiality procedures;
- * Training pastors, staff, ministry leaders, and volunteers where appropriate;
- * Limiting access to personal information;
- * Reviewing vendors and service providers;
- * Maintaining secure systems and records;
- * Using appropriate consent forms;
- * Maintaining incident response procedures;
- * Reviewing children's and youth privacy practices;
- * Reviewing donor and financial information practices;
- * Reviewing this Privacy Notice periodically.

The Church should review its privacy practices whenever it launches a new website, app, online giving platform, youth program, digital ministry, livestreaming process, counseling ministry, or major event registration system.

This Privacy Notice may be supported by additional procedures, forms, consent notices, confidentiality agreements, breach response protocols, donor privacy statements, children and youth ministry notices, and volunteer screening notices, as appropriate to the Church's ministry activities.

26. Practical New York Implementation Recommendations

To support this Privacy Notice, the Church should consider adopting the following New York-focused supporting documents and practices.

26.1 New York Data Breach Response Procedure

The Church should maintain a written breach response procedure that includes:

- * Who must be notified internally;
- * How incidents should be documented;
- * How vendors should report incidents;
- * When legal counsel should be contacted;
- * How New York notification obligations will be assessed;
- * How affected individuals will be notified where required;
- * How appropriate New York authorities will be notified where required;
- * How records of decisions will be maintained;
- * How post-incident improvements will be made.

26.2 New York Reasonable Safeguards Checklist

The Church should maintain a safeguards checklist that covers:

- * Administrative safeguards;
- * Technical safeguards;
- * Physical safeguards;
- * Vendor safeguards;
- * Secure disposal;
- * Training;
- * Risk review;
- * Access control;
- * Incident response.

This checklist should be reviewed periodically and whenever the Church adopts a new system or begins a new ministry activity involving personal information.

26.3 Children and Youth Registration Form

The Church should use a children and youth registration form that includes:

- * Parent or guardian consent;
- * Emergency contact information;
- * Medical, allergy, dietary, or accommodation information;
- * Transportation permission;
- * Check-in/check-out rules;
- * Media consent;
- * Authorization for emergency care where appropriate;
- * Contact preferences.

26.4 Media Release Form

The Church should use a media release form for:

- * Adults;
- * Children and youth, signed by a parent or guardian;
- * Testimonies;
- * Promotional videos;
- * Livestream participation;
- * Published photographs;
- * Special events, camps, retreats, and conferences.

26.5 Volunteer Confidentiality Agreement

The Church should require confidentiality commitments from volunteers and ministry workers who access:

- * Children's or youth information;
- * Membership records;
- * Donor records;
- * Prayer requests;
- * Pastoral care information;
- * Benevolence records;
- * Health or emergency information;
- * Financial information;
- * Background check records.

26.6 Donor Privacy Statement

The Church should publish or include a short donor privacy statement on giving pages and donation forms explaining:

- * How donor information is used;
- * Whether donor information is shared;
- * That donor lists are not sold;
- * How receipts are issued;
- * How donors may update contact preferences.

26.7 SMS/Text Consent Wording

For SMS or text messaging, the Church should use clear consent wording, especially for:

- * Youth ministry updates;
- * Event reminders;
- * Fundraising campaigns;
- * Devotionals;
- * Emergency notices;
- * Volunteer coordination.

Consent wording should explain the type of messages, the frequency where possible, and the opt-out method.

26.8 Website Cookie and Tracking Notice

If the Church uses cookies, analytics, pixels, app tracking, or targeted advertising tools, the Church should publish a website cookie notice explaining:

- * What tools are used;
- * Why they are used;
- * Whether third parties receive information;
- * How users can control cookies or tracking.

The Church should seek legal review before using targeted advertising, retargeting pixels, or data-sharing tools that involve sensitive information related to church participation, donors, youth, pastoral care, or prayer.

27. Changes to This Privacy Notice

The Church may update this Privacy Notice from time to time to reflect changes in ministry activities, technology, legal obligations, or privacy practices.

The updated Privacy Notice will be posted on the Church's website, app, office noticeboard, or other appropriate location.

The "Last Updated" date will show when the Privacy Notice was most recently revised.

28. Contact Us

If you have questions, concerns, or requests about this Privacy Notice or how your personal information is handled, please contact:

[Insert Church Name]

Address: [Insert New York Address]

Email: [Insert Privacy Contact Email]

Telephone: [Insert Telephone Number]

Privacy Contact / Responsible Officer: [Insert Name or Office]

We encourage individuals to contact the Church first so that privacy concerns can be addressed promptly, respectfully, and appropriately.