Friendship Church
Data Security Notification and Confidentiality Policy

Owner:	Lead Pastor
Effective Date:	July 1, 2020
Latest Revision Date:	July 1, 2020

Purpose

Friendship Church (FC) recognizes its need to maintain the confidentiality of Personal Identity Information (PII) and Protected Health Information (PHI), and understands that such information is unique to everyone; whether a visitor, regular attendee, or member. The PII/PHI covered by this policy may come from various types of individuals performing tasks on behalf of the church and includes employees, volunteers, independent contractors, and any PII/PHI maintained in electronic and non-electronic forms. The scope of this policy is intended to be comprehensive and will include FC requirements for the security and protection of such information throughout the company and its approved vendors, both on and off work premises.

The security of our attendees' and visitors' data is of crucial importance. We never sell or share individuals' information with third parties.

The applications we use for electronic data storage use industry standard 256-bit encryption to protect our communication with its servers.

Our data is backed up each night at a secure data center, where the employees undergo background checks. Additionally, the online giving products we use are Level 1 PCI Compliant. This means that they've earned the highest level of accreditation possible for online giving security. We hope this exemplifies our commitment to data privacy and the security of sensitive information.

Physical (non-electronic) data may be stored in a variety of forms including photographs, film, optical media (e.g. CDs & DVDs), magnetic media (e.g. audio and video tapes or computer storage devices), artworks, paper documents or computer printouts.

All physical data collected by Friendship Church is kept in secure storage, such as a locked storage room or locked filing cabinet within the church or church offices. Only the Lead Pastor and Associate Pastor have access to this information.

As an individual performing tasks on behalf of the church it is critical you understand the importance of how FC protects data and the legal requirements to not share data that may be shared with you from a member, attendee and/or visitor of FC.

Personally Identifiable Information (PII)

PII or personally identifiable information is any data that can be used to contact, locate, or identify a specific individual, either by itself or combined with other sources that are easily accessed. It can include information that is linked to an individual through financial, medical, educational or employment records. Some of the data elements that might be used to identify a certain person could consist of fingerprints, biometric data, a name, telephone number, email address or social security number. The protection of PII is essential for all organizations. Some of the laws that are related to different forms of PII include: HIPAA, Privacy Act, GLBA, FERPA, COPPA, and FCRA. These laws are utilized as an important way of attempting to ensure that organizations are restricted from sharing personal information with other parties. They also provide requirements for protecting that information in the most appropriate manner.

Examples of PII

- A personal identification number, such as a driver's license number, passport number, patient identification number, credit card number or social security number.
- A name, including the full name of the individual, their maiden name or mother's maiden name, and any alias they may use.
- Address information, like email addresses or street addresses, and telephone numbers for businesses or personal means.
- Biological or personal characteristics, such as an image of distinguishing features, fingerprints, x-rays, voice signature, retina scan, or geometry of the face.
- Information about an individual that is linked to their place of birth, date of birth, religion, activities, geographical indicators, educational, financial, or medical data.

Protected Health Information

HIPAA, or the Health insurance portability and accountability act, has required certain security regulations to be adopted for protected health information. Often, PHI is regarded to be any health information that is individually identifiable, and created or received by a provider of health care, a health plan operator, or health clearing house. The information might be related to an individual's present, past or future health, either in physical or mental terms, as well as the current condition of a person. Generally, PHI can be used to identify a specific individual, and it refers to data that is either maintained or transmitted in any given form, including speech, paper, or electronics.
PHI does not refer to the education records that are covered by the educational family rights and privacy act. Nor does it refer to any employment records that are maintained

by a covered entity as that entity's role as a person's employer. The regulations typically refer to several different fields which might be utilized to identify a person, including:

- Names
- All dates directly linked to an individual, including date of birth, death, discharge, and administration.
- Telephone and fax numbers
- Email addresses and geographic subdivisions such as street addresses, zip codes and county.
- Medical record numbers, and health plan beneficiary numbers.
- Certificate numbers or account numbers
- Social security numbers, or vehicle identifiers
- Biometric identifiers, including voice or finger prints.
- Photographic images of the full face or recognizable features
- Any unique number-based code or characteristic

What is a data breach?

A data breach is an incident that exposes confidential or protected information. A data breach might involve the loss or theft of a Social Security number, bank account or credit card number, personal health information, passwords, or email.

A data breach can be intentional or accidental. A cybercriminal may hack a computer system storing personal information; or an individual at an organization may accidentally expose information on the internet or to another individual. Either way, data breaches create risks for the individual and the organization.

What if a data breach occurs?

The Lead Pastor serves as the Privacy Officer. Should you become aware of a data breach (verbally, electronically or paper), you must notify the Lead Pastor immediately, so appropriate actions can be taken.

Violation of Policy:

Individuals performing tasks on behalf of the church, both employees and volunteers, are required to adhere to this policy. Consequences for violating this policy include:

- **First Offense:** a verbal reprimand will be given, with a note placed in a file with the time and date of conversation, signed by the Team Leader and/or Director.
- **Second Offense:** a written reprimand to the violator, signed by the Team Leader and/or Director.
- **Third Offense:** the violator will be disqualified from participating in tasks on behalf of the church.

How do we manage this policy?

This policy is posted on the FC website and is stored electronically. The Lead Pastor serves as the Privacy Officer and will review and update this policy at least once a year.

By reading and signing this policy I agree I:

- have read and understand this policy in its entirety
- have read and understand the definitions of PII and PHI
- understand how FC manages and stores data for its members, attendees, and visitors
- understand what a data breach is and what to do if one occurs
- will not share information given or gathered from FC members, attendees, and visitors of FC, in any manner (verbally, paper or electronically)
- understand the consequences of violating this policy

Employee or Volunteer:	**Privacy Officer:**
_____	_____Mark Crawford_____
Printed Name	Printed Name
_____	_____
Signature	Signature
_____	_____
Date	Date

FC
CARE MINISTRIES