SAINT ANDREW CATHOLIC CHURCH

Newtown, Pennsylvania

Data Protection Policy
November 2015

Saint Andrew Catholic Church Data Protection Policy

Saint Andrew Catholic Church of Newtown, Pennsylvania is committed to respecting and protecting the confidentiality of personally identifiable information relating to its parishioners, pupils, parents and staff accumulated through the operation of the Church's various ministries.

1. Introduction

a. The Parish of Saint Andrew collects and uses personally identifiable information about the parishioners, the school's pupils and parents, office staff and volunteers, and other individuals who come into contact with the Parish's ministries. This information is gathered in order to enable the Parish to provide services, education and other related functions pertaining to the operation of the Parish.

b. This policy is intended to ensure that personally identifiable information is handled correctly, securely and used only for its intended purposes, and to assure the parties involved that their personally identifiable information is protected.

c. All staff involved in the collection, processing and disclosure of personally identifiable information will be aware of their duties and responsibilities regarding the protection of the personally identifiable information collected and/or produced in the course of performing their duties.

2. What is Personally Identifiable Information?

Personally identifiable information is defined as data which relates to a living individual who can be identified from that data by itself or in combination with other data.

a. For example, a person's name, by itself, does not constitute personally identifiable information. However, if a person's name and address, or social security number, or telephone number or email address are presented together, that combination reflects personally identifiable information since it can be used to identify a specific person.

b. If personally identifiable information is presented in a printed report, or merely displayed on a computer screen, both presentations are to be treated as confidential information by the possessor of the information and must be protected against unauthorized access.

c. Another example is a student's name by itself on a class roster does not necessarily represent personally identifiable information. However, a student's name on a bus schedule would constitute personally identifiable information since that combination could be used to determine the residence and, thus, identity of the student.

3. General Statement

Because Saint Andrew Catholic Church is committed to protecting the confidentiality of personally identifiable information relating to its parishioners, its school's pupils and parents, and its various support staffs and volunteers, the parish will:

a. Ensure that clear and robust safeguards are in place to protect personally identifiable information from unauthorized disclosure,

b. Share information with others only when it is legally required to do so and that such requests are formally submitted in writing, reviewed and approved by the senior staff person of the particular parish activity (for example, for the school, the school's principal; for the parish's administrative office, the parish business manager),

c. Develop internal procedures to ensure that when personally identifiable information is extracted from the parish's computer systems, whether in the form of printed reports or screen displays, that the information is treated confidentially and disposed of in a secure manner,

d. Ensure that the office/support/ministries staffs are aware of and understand this policy.

4. Rights to Access Personally Identifiable Information

a. All parishioners, staff, school faculty and volunteers, and parents are entitled to:
    i. Know what information the parish holds and processes about them or their child and why,
    ii. Know how to gain access to their data,
    iii. Know how to keep their data up to date and
    iv. Know what data may be made available to agencies external to the parish.

b. The parish will comply with formally documented requests for access to personally identifiable information directed by the Philadelphia Archdiocese and by appropriate governmental agencies.

c. Personally identifiable information may be shared with third party organizations, such as state agencies (for example, for provided medical services history for the school's students through the school's nurse's office), or for companies providing services to the parish such as bus transportation and catering services for the school.

5. Third Party Services Providers

The parish may use third party service providers to manage its data collection, storage and information processing services. The parish ensures that any such agreements for services

will include contractual language that guarantee the existence of suitable precautions to safeguard the data entrusted in their care. Specifically:

a. The parish will always remain the owner of the data.

b. The service provider is not entitled to use any parish-related data held on its systems for any purpose other than to provide the required services to the parish.

c. The service provider is required to take industry-standard precautions to ensure the security and confidentiality of the data residing in their systems.

d. The parish, once it terminates its agreement with the service provider, any and all parish-related data held in the provider's systems will be completely purged and not used for any other purpose. The service provider will be required to acknowledge and attest to this purging formally in writing.

6. **Specific Responsibilities for Office Staff/School Faculty With Access Rights to Personally Identifiable Information**

a. Access to the parish's databases and hard copy personnel files will be on a need to know basis, and such access rights will be subject to approval at the facility's manager (for example, school principal or parish office business manager) and higher management levels only.

b. With regard to personnel records, particularly on matters of staff and volunteers' security and youth protection clearances, facility managers must develop and monitor compliance of procedures designed to protect the confidentiality of this type of personally identifiable information.

c. With regard to school operation, the school's principal will, prior to the start of a new school year, perform an annual review of access rights to the school's student information systems granted to staff and faculty. Any changes in access rights are to be reported to the school's computer systems manager for application as soon as possible.

d. Standard computer access controls will be in place to include:
    i. requiring electronic authentication via the use of a valid username and password for all who are granted access to the parish's information systems,
    ii. changing of user passwords, at least annually, for school staff and faculty who access the school's information systems and
    iii. activating computer screen timeouts automatically after 30 minutes or so of inactivity and, when re-activated, requiring user re-authentication.

e. Computer users **must not leave** their computer unattended if the computer is logged onto the parish or school's database systems (for example, ACS or RenWeb).

f. The parish uses a third party service to provide document shredding services of sensitive reports and documents of no further use to parish's staff and school's faculty. Storage bins have been installed in specific locations at the parish office and school specifically to store such documents until they are properly destroyed.

   i. Staff and faculty personnel who produce, through the school's information systems, any report which includes personally identifiable information must advise any recipient of the report of the sensitive nature of the report and instruct the recipient on the proper method of disposing of the report at the end of its usefulness.

   ii. Staff, volunteers and school faculty personnel receiving a report which includes personally identifiable information must, at the end of the report's useful life, place the report into the storage bins set aside specifically for shredding.

   iii. The parish's policy in this matter is simple: **There is to be no casual discarding of printed reports containing personally identifiable information derived from data accumulated through the parish's information systems**. Office staff and school staff/faculty must be vigilant in their individual efforts at insuring the proper, secure handling and disposal of such printed reports in their care.

g. **Please Note:** Willful failure to comply with this policy and, thus, causing accidental or purposeful breach the parish's personally identifiable information protection policy may lead to disciplinary action up to and including termination of employment or volunteer status. Any remedial action will be proposed by the senior staff person of the particular parish activity (for example, for the school, the school's principal; for the parish's administrative office, the parish business manager) and subject to approval by the pastor of Saint Andrew Catholic Church. (Additional Note: In some situations of breach, particularly involving disclosure of clearance-related personal information, such a breach may be subject to criminal investigation and prosecution.)

7. Retention of Data

The parish has an obligation to retain parishioner, school pupil and parent, and staff personal data for an indefinite period of time following their departure from the parish or school, mainly for legal reasons for the school, but also for other purposes such as being able to provide references and sacramental documentation.