PRIVACY AND SENSITIVE INFORMATION POLICY & PROCEDURES

PURPOSE: To comply with California laws and good ethical conduct practices in the protection of personal and the Church information.

BACKGROUND & DEFINITIONS:

1. **The California Online Privacy Protection Act of 2003 (OPPA) effective 7/1/04** states that operators of commercial websites that collect personally identifiable information from California's residents are required to conspicuously post and comply with a privacy policy that meets certain requirements.

   According to the act, the operator of a website must post a distinctive and easily-found link to the website's privacy policy. The privacy policy must detail kinds of information gathered by the website, how the information may be shared with other parties, and if such a process exists, describe the process the user can use to review and make changes to their stored information. It must also include the policy's effective date and a description of any changes since then.

2. **Information Practices Act of 1977, California**

   Article 1: General Provisions and Legislative Findings: chapter 1798.1: The legislature declares that the right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them.

   Article 2: Definitions: chapter 1797.3: As used in this chapter:
   The term "personal information" means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual…
   The term "disclose" means to disclose, release, transfer, disseminate, or otherwise communicate all or any part of any record orally, in writing, or by electronic or any other means to any person or entity.

   Article 5: Agency Requirements:
   Chapter 1798.14: Each agency shall maintain in its records only personal information which is relevant and necessary to accomplish a purpose of the agency required or authorized by the California Constitution or statute or mandated by the federal government.

   Chapter 1798.20: Each agency shall establish rules of conduct for persons involved in the design, development, operation, disclosure, or maintenance of records containing personal information and instruct each such person with respect to such rules and the

requirements of this chapter, including any other rules and procedures adopted pursuant to this chapter and the remedies and penalties for noncompliance.

Chapter 1798.21: Each agency shall establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the provisions of this chapter, to ensure the security and confidentiality or records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury.

Chapter 1798.22: Each agency shall designate an agency employee to be responsible for ensuring that the agency complies with all of the provisions of this chapter.

Article 6: Conditions of Disclosure:
Chapter 1798.24: No agency may disclose any personal information in a manner that would link the information disclosed to the individual to whom it pertains…. [Exceptions to this rule are listed in the statute.]

Article 10: Penalties:
Chapter 1798.55: The intentional violation of any provision of this chapter or any rules or regulations adopted there under, by an officer or employee of any agency shall constitute a cause for discipline, including termination of employment.

Chapter 1798.56: Any person who willfully requests or obtains any record containing personal information from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than five thousand dollars ($5,000), or imprisoned not more than one year, or both.

3. Information Categories

a. Public Information. This information has been formally approved for public release and must be protected against alteration of its official source. Examples include scriptures, curriculum materials, news releases and official information about the Church and its doctrines.

b. Internal Use Only. This information is generally accessible within the Church but not intended for external entities or persons. Internal use information may have additional handling or access control requirements. Examples include most e-mail and other correspondence and documents, organization charts, employee work, e-mail addresses, and telephone numbers and most software.

c. Confidential Information. This information requires special handling and controls specific to the use of the information and work environment. Examples include most information about people such as salary and performance information, member personal and medical information, organizational plans, strategies and changes that have not been decided and announced, and most organization financial information.

d. Restricted Information. Confidentiality and integrity risks are very high and a failure in protection could have severe repercussions. Access is tightly restricted with the most stringent security safeguards at the system and user level. Examples include payment (credit and debit) card information, encryption keys, passwords, disciplinary records, financial information aggregated above department level, and very sensitive general authority communications.

POLICY/PROCEDURES

1. **Compliance with laws and regulations.** All persons responsible for or having access to privacy and confidentiality information will:
   a. Comply with The California Online Privacy Protection Act of 2003 (OPPA)
   b. Comply with the California Information Practices Act of 1977, California

2. **Individual responsibility**
   a. Pastors, managers, employees and volunteers given access to the Church private and confidential information must take personal responsibility for appropriately protecting the information, for applying the controls and conditions defined for its use, and for reporting apparent breaches in handling controls and use conditions.

   b. A person given access is responsible for safeguarding the private and confidential information obtained during employment or volunteer service at the Church. In the course of efforts, he/she may have access to privacy and confidential information regarding the Church, its suppliers, its members, or employees and volunteers. He/she has responsibility to prevent revealing or divulging any such private and confidential information unless it is necessary for you to do so in the performance of your duties. Access to private and confidential information should be on a "need-to-know" basis and must be authorized by your supervisor. Any breach of this policy will not be tolerated by the Church, and the employee may be subject to disciplinary action, up to and including termination

   c. A supervisor must understand their obligation to orient a person under their supervision to ensure that she/he understands the state and federal laws and the Church Privacy and Confidential Information Policy that governs access to and use of personal/confidential information.

   d. A person with access must comply with the state and federal laws and Church policies that govern access to and use of information contained in employee and volunteer, applicant, and member records, including data that is accessible through the Human Resources information system.

e. A person granted access to information and/or data is strictly limited to access to the specific information and data that is relevant and necessary for them to perform their job related duties.

f. A person given access is prohibited from accessing information or data that is not relevant and necessary for them to perform their job-related duties.

g. A person given access must agree to be a responsible user of information and data, whether it relates to his/her own department or another department.

h. A person given access must maintain the privacy and confidentiality of the information and data he/she obtains in an accurate and professional manner.

i. Before sharing information or data with others, electronically or otherwise, a person given access must ensure that the recipient is authorized to receive the information or data and understands his/her responsibilities as a user.

j. A person with access must sign off on any computerized system when they are not actively using it.

k. A person with access must keep their password (s) to themselves, and will not disclose them to others unless their immediate supervisor authorizes such a disclosure in writing.

l. A person with access must store and secure confidential and sensitive information, data, reports, etc. in a manner that will maintain its confidentiality when they are not actively using them.

m. A person with access must dispose of confidential reports in a manner that will preserve its confidentiality when they have finished using it.

3. **Information Obtained From a Hospitalized Patient or Family Member.** The HIPAA laws for patient's privacy in CA have changed to include fines for clergy who knowingly or unknowingly violate someone's privacy. It is the Church's policy that any employee visiting a patient or family member in the hospital must follow the procedures outlined in the policy entitled "Hospitalized Patient Privacy Policy."

4. **Responsibilities for Shared Information Repositories**. When information is in a common repository for shared use, such as a database or data warehouse, the person responsible for that repository must adhere to access and handling controls and use conditions established for the information by the IT manager. Repository management must also support any new controls that are appropriate due to the increased sensitivity resulting from the expanded information combinations and aggregations the repository makes possible.

5. **Computer Password protection.** All Church computers are to be password protected at all times.
6. **Church Labeling of Sensitive Information.** Procedures, stamps/labeling tools and computer labeling procedures as needed must be used to properly mark and store "Private and Confidential Information" with the following labels as appropriate: Private Information, Internal Use Only, Confidential Material and Restricted Information.
7. **Website Privacy.** The operator of the Church website must post a distinctive and easily-found brief statement and link to the website's privacy policy
8. **Media Contact**. Employees and volunteers may be approached for interviews or comments by the news media. All media requests should be referred to our _____, who has been designated by the Senior Pastor and _____ to comment on Church policy or events that have an impact on the Church. The _____ will notify the Senior Pastor and others as stipulated by procedure.
    a. Let the reporter know that the _____ will return their call, if possible, within the hour or by the end of the day.
    b. Be courteous and ask the reporter for their name, news organization, phone number, and deadline.
    c. Under no circumstances should you feel obligated to respond to a news reporter's questions or confirm information.
    d. Failure to follow the above process may subject you to disciplinary action up to and including termination.