

## **VIII. Illinois Biometric Information Security Policy**

If you are an Illinois resident and The Church collects, uses, or discloses biometric data, this policy may apply to you.

### **A. Purpose**

This Biometric Information Security Policy (the “BIS Policy”) defines The Church’s policy and procedures for collection, use, safeguarding, storage, retention, and destruction of biometric data collected by The Church.

The Church collects passport photographs via applications for Activities on its website to ensure that you are eligible to travel internationally for Activities and to have a picture of you in the event it is necessary for identification or other purposes. Collection of passport photographs may allow geometric or other scanning of your face in the photograph.

### **B. Definition of Biometric Data**

The terms “biometric data” and “biometric information” as used in this BIS Policy and Release, Consent and Indemnity Agreement, are intended to have the same definition provided in the Illinois Biometric Information Privacy Act, 740 ILCS §14/1, *et seq.*

### **C. BIS Policy**

The Church’s policy is to protect and store biometric data in accordance with the applicable standards and laws, including the Illinois Biometric Information Privacy Act. An individual’s biometric data will not be collected or otherwise obtained by The Church without prior written consent of the individual. The Church will inform the individual of the reason his or her biometric information is being collected and the length of time the data will be stored.

The Church will not sell, lease, trade, or otherwise profit from an individual’s biometric data. Biometric data will not be disclosed by The Church unless (i) consent is obtained, (ii) required by law; or (iii) required by valid subpoena or warrant.

Biometric data will be stored during the term of your application for, and participation in, Activities. The biometric data will be stored using a reasonable standard of care and in a manner that is the same or exceeds the standards used to protect other confidential and sensitive information held by The Church. For example, these safeguards include physical and digital security measures, encryption, access restrictions, password authorization, system logging, and file backup.

The Church will permanently destroy your biometric data when the first of the following occurs:

- a. The initial purpose for collecting or obtaining such biometric data has been satisfied, such as your return home from all Activities and statement that you do not plan to participate in any additional Activities; or
- b. Within two (2) years of the last Activities in which you participated.