



COMPLIANCE & DATA GOVERNANCE

Data & Privacy Guidelines

Consent, Security, and Responsible Documentation

DOCUMENT

BSC-COMP-001

VERSION

Version 1.0

ISSUED

Issue Date: June 2026

For Use by Authorized The BSC Ministry Team Members

CITY OF REFUGE BIBLE STUDY CENTER

A Program of Alliance for Population Health (APHA), Inc.

DOCUMENT CONTENTS

Table of Contents

01	Our Commitment to Privacy
02	Foundational Principles
03	What Data The BSC Collects
04	Consent: The Non-Negotiable
05	How Data Is Stored & Secured
06	Who Has Access
07	Public-Facing Data
08	Data Retention & Removal
09	Incident Response
10	Team Member Responsibilities

SECTION 01

Our Commitment to Privacy

The City of Refuge Bible Study Center (The BSC) is committed to handling personal data with the highest standards of consent, security, and respect — at all times, in all contexts, with no exceptions.

As a program of Alliance for Population Health (APHA), Inc. — an organization with deep expertise in monitoring, evaluation, and community health programming — The BSC applies the same data discipline that governs international public health work to the data we collect in Christian ministry. The standards are professional. The motivation is pastoral. The result is trustworthy.

"He that walketh uprightly walketh surely: but he that perverteth his ways shall be known."

— Proverbs 10:9 (KJV)

This document is binding on every The BSC team member who handles personal data in any form. By logging in to the Impact Registry or recording any information from an outreach encounter, you affirm that you have read, understood, and will abide by these guidelines.

SECTION 02

Foundational Principles

Five principles govern every aspect of The BSC's approach to personal data. These principles are not negotiable and supersede convenience, efficiency, or individual preference.

1**Consent**

No personal data is collected, stored, or used without the informed consent of the individual. Consent is asked, not assumed.

2**Minimization**

We collect only what is genuinely needed for ministry care. If we do not need a piece of information to follow up well, we do not collect it.

3**Security**

All data is stored in encrypted, password-protected systems. It is never shared, sold, traded, or exposed to third parties.

4**Transparency**

Individuals can ask at any time what data we hold about them, how it is used, and request its removal.

5**Stewardship**

Every record represents a real human being. Data is handled with the dignity that human beings deserve.

SECTION 03

What Data The BSC Collects

The BSC collects only the data necessary for meaningful pastoral follow-up. The following table specifies what is collected and what is explicitly NOT collected.

CATEGORY	COLLECTED	NOT COLLECTED
Identity	First name (optional)	Full legal name, ID numbers, SSN, DOB
Contact	Phone or email (only if person consents to follow-up)	Home address, family member contact details
Location	Community, neighborhood, or city of encounter	Specific street address unless person consents
Encounter	Date, outreach method, brief context	Verbatim conversation transcripts
Spiritual	Decision noted (e.g., prayer received, openness expressed)	Theological judgments, doubts, or personal critiques
Sensitive	Only with explicit consent and clear pastoral need	Health, finance, legal, family conflict — unless required for care

When In Doubt

If you ever find yourself asking, "Should I record this?" — the default answer is no. Record less, not more. Privacy protected is harder to undo than data uncollected.

SECTION 04

Consent: The Non-Negotiable

Consent is the foundation of all data collection. It is not a formality. It is a spiritual and ethical obligation.

What Genuine Consent Looks Like

- **Informed.** The person knows what is being recorded and why.
- **Voluntary.** The person can refuse without consequence to the ministry encounter.
- **Specific.** Consent for follow-up by phone is not consent to share their data with a partner organization.
- **Revocable.** The person can withdraw consent at any time and we will honor it.

How to Ask for Consent

Use plain language. Avoid legal jargon. A simple, honest conversation works best:

"I'd love to stay in touch and keep praying for you. Would you be okay if I logged a quick note in our system — just your first name, the fact that we met today, and your phone number — so I can check in with you in about a week? Your information stays private to our team — we don't share it with anyone outside The BSC. You can ask me to remove it any time."

When Consent Cannot Be Obtained

If for any reason you cannot ask for or obtain consent — the person is in crisis, the conversation ended abruptly, or the context did not allow for it — you may still record an anonymous encounter (date, location, brief context, no identifying details). You may not record contact information, names, or follow-up details without consent.

SECTION 05

How Data Is Stored & Secured

All personal data collected by The BSC is stored in the Impact Registry — a password-protected database accessible only via authenticated session.

Technical Safeguards

- **Encrypted at rest.** All data stored in the Impact Registry is encrypted on the database server.
- **Encrypted in transit.** All data sent between your device and the registry uses HTTPS/TLS encryption.
- **Authentication required.** No data is viewable without a valid login.
- **Role-based access.** Different team roles see different levels of data. Team members see only what they need for their work.
- **No third-party tracking.** The BSC does not allow any third-party marketing, analytics, or advertising trackers on data systems.

Operational Safeguards

- **Unique credentials.** Each team member has their own login. Sharing credentials is prohibited.
- **Strong passwords.** Minimum 12 characters, mix of letters, numbers, symbols. Recommend a password manager.
- **Auto-logout.** Sessions expire after periods of inactivity.
- **Audit logs.** The system logs who accesses what records and when. Suspicious activity is reviewed.
- **Regular backups.** Data is backed up regularly so no record is permanently lost.

SECTION 06

Who Has Access to The BSC Data

ROLE	ACCESS LEVEL
Outreach Team Member	Records they personally created; their assigned follow-up queue. Cannot see other team members' records.
Team Coordinator	All records for their assigned community or geographic area. Can reassign follow-ups and view team activity.
The BSC Administrator	Full access to all records for reporting, analytics, and operational oversight. Limited to authorized administrative staff.
APHA Leadership	Aggregate reports and anonymized analytics only. Does not access individual personal records unless a specific oversight need arises.
General Public	No access to personal data. May view only anonymized community-level aggregates via the public Community Impact Map.
Third Parties	No access. Personal data is never shared with third parties under any circumstances except where required by law (see Section 09).

SECTION 07

Public-Facing Data

The BSC website displays certain data publicly to build credibility, communicate impact, and inspire continued engagement. All public-facing data is aggregated and anonymized — no personal information is ever exposed.

What Appears Publicly

- **Total community count** — number of communities reached, no names.
- **Geographic visualization** — community-level pins on the Impact Map, no addresses, no names.
- **Aggregate milestones** — "Together we have prayed with X individuals," with no individual identification.
- **Article and study content** — fully public, intentionally so.
- **Prayer Map prayer requests** — only those submitted with explicit consent for public visibility; otherwise anonymous.

What Never Appears Publicly

- Names, even first names
- Contact information of any kind
- Specific street addresses
- Photos or images of individuals reached
- Spiritual decisions tied to identifiable individuals
- Follow-up notes or pastoral records

SECTION 08

Data Retention & Removal

Records in the Impact Registry are retained as long as they serve active ministry purpose. Records are not held indefinitely without reason.

Standard Retention

Active follow-up records are retained for the duration of the relationship plus a reasonable archival period (typically 2 years after the last contact) for operational continuity and audit purposes. After this, records are either archived or anonymized.

Individual Right to Removal

Any individual whose data is held by The BSC has the right to request its removal at any time. The process:

1**Request**

Individual contacts The BSC Team Lead via the contact information at the back of this document, or through the Contact page of The BSC website.

2**Verification**

We confirm the individual's identity to ensure we are not removing the wrong record or acting on a malicious request.

3**Action**

The record is removed from the Impact Registry within 30 calendar days. Anonymized aggregate data (which contains no personal identifiers) may remain in historical reports.

4**Confirmation**

We confirm completion to the individual in writing.

SECTION 09

Incident Response

In the event of a suspected data breach, unauthorized access, lost device, or any incident that may compromise personal data, the following response is mandatory.

1

Notify Immediately

Notify The BSC Team Lead within one hour of becoming aware of the incident. Do not delay to investigate yourself first.

2

Contain

If a device is lost or stolen, remotely lock or wipe it. Change account passwords. The BSC Team Lead will revoke compromised credentials immediately.

3

Assess

The Team Lead, in consultation with APHA leadership, will assess the scope of the incident: what data, whose data, how exposed, what remediation is needed.

4

Notify Affected Individuals

If individuals' personal data was or may have been exposed, those individuals will be notified directly within a reasonable timeframe — typically 7–14 days depending on the scope and nature of the incident.

5

Remediate & Document

Implement corrective actions to prevent recurrence. Document the incident, the response, and the outcome in The BSC's internal incident log.

Mandatory Reporting

Failing to report a known or suspected incident is itself a breach of these guidelines. There will be no penalty for honest, prompt reporting — even if the incident was caused by your own mistake. There will be consequences for concealment.

SECTION 10

Team Member Responsibilities

Every The BSC team member who handles personal data is personally responsible for upholding these guidelines. The following commitments apply to all team members at all times:

- I will **obtain consent** before logging any personally identifying information.
- I will **minimize** the data I collect to only what is needed for genuine ministry care.
- I will **not share** Impact Registry login credentials with anyone, ever.
- I will **use strong passwords** and never write them down where others can see.
- I will **not screenshot, photograph, or copy** personal data from the Impact Registry to any external device, app, or system.
- I will **not discuss** identifiable personal information about people in The BSC's care with friends, family, or outside parties.
- I will **report incidents** immediately, without delay or concealment.
- I will **honor removal requests** promptly and without resistance.
- I will **treat every record** as if it were a record about my own family member.

"He that is faithful in that which is least is faithful also in much..."

— Luke 16:10 (KJV)

Acknowledgment

By logging into the Impact Registry or by recording any personal data on behalf of The BSC, you acknowledge that you have read, understood, and agree to abide by these Data & Privacy Guidelines in full.

QUESTIONS OR SUPPORT

Bolaji Fapohunda, Team Lead

City of Refuge Bible Study Center (The BSC)

Phone: 240.204.3890

Email: Bolaji.fapohunda8@gmail.com