Using Switchboard With Security in Mind

Understanding Security on Switchboard

Switchboard is designed to help workers connect with skilled volunteers while keeping security in mind.

While no platform can be completely secure, Switchboard uses industry best practices, including encryption, hashing and separate off-platform validation for personal identifiers. Users can control the level of detail they share in their profiles and requests and, if they choose, use a pseudonym to enhance anonymity. Additionally, the full details of a request are only visible to volunteers who have created a profile on Switchboard.

Minimizing Risk

Switchboard is designed with security in mind, but like any online platform, it is only as secure as the information users provide. Security is ultimately the responsibility of the individual posting the need, so it’s important to be intentional of the information you share and follow best practices to minimize risk.

- **Follow your organization’s protocols** for public communication.
- **Use broad terms** when posting a need in a restricted-access area, avoid mentioning full names, exact locations, details about your ministry partners, or any information that could point to a specific place.
- **Always use secure communication methods,** such as encrypted messaging apps or secure email, for follow-up conversations with volunteers off of the Switchboard platform.
- **Monitor and adjust** your posts as needed. If concerns arise, you can edit or remove your request at any time.

For those in extremely high-risk areas, we also advise consulting security professionals before using Switchboard.

Be Proactive, Stay Secure

Security is an ongoing process. By being mindful of what you share and using the platform wisely, you can safely connect with skilled volunteers while protecting your ministry.

info@globalswitchboard.io

Developed through a MissioNexus Innovation grant by:

Switchboard CHRISTAR PIONEERS