Area 15 Airtable Data Privacy Guidelines

1. Purpose and Scope
The purpose of the Area 15 Airtable database is to maintain accurate group and service contact records to facilitate essential communication within Area 15. This data is collected strictly for administrative and service-related purposes. These guidelines apply to all District Registrars and any trusted servants granted access to the Area 15 Airtable.

2. Privacy and Confidentiality
Protecting the personal data of our members is a matter of strict privacy and confidentiality. The trust of the fellowship relies on our ability to safeguard this information. The data stored within this database, including full names, phone numbers, email addresses, and physical addresses, is highly confidential. It is collected solely for the purpose of carrying out Area 15 service work and must never be treated casually, shared with, or viewed by unauthorized individuals.

3. Access Controls
- **Authorized Trusted Servants Only:** Access to the Area Airtable is restricted exclusively to current District Registrars and the Area Registrar and read-only access to the Area 15 Chair.
- **Individual Licenses:** Area 15 funds an Airtable license and access for each active District Registrar. Registrars must access Airtable using their own dedicated login credentials. Account sharing or sharing passwords is strictly prohibited.
- **Access Revocation:** Upon rotating out of the District Registrar position, the outgoing registrar must immediately notify the Area Registrar so their Airtable access can be discontinued. That district's license is then reassigned to the incoming District Registrar.

4. Strict Prohibition on Data Sharing
- **No External Sharing:** District Registrars are **strictly prohibited** from sharing, distributing, selling, or otherwise disclosing any personal information found in the Airtable database to anyone.
- **Internal Communication Only:** Contact information may only be used for official Area/District AA business. It must never be used for personal reasons, solicitation, or non-AA related announcements.
- **BCC for Emails:** When using emails sourced from the database to contact multiple members, Registrars must always use the BCC (Blind Carbon Copy) field to prevent exposing members' email addresses to one another.

5. Airtable Security & Data Handling
- **Device Security:** Registrars must only access the database on secure, password-protected computers or devices. Registrars must never leave the Airtable database open on a public or shared computer.
- **Exporting and Downloading:** Downloading or exporting Airtable data that contains the personal information of members (e.g., to Excel or CSV files) should be avoided. Any downloaded data must be stored securely and permanently deleted from the user's device immediately after the task is completed.
- **No Public Links:** Registrars must never create or share "Public View" links from Airtable that could expose member data.

6. Incident Reporting
If a Registrar suspects that data has been accidentally shared, downloaded to an insecure location, or accessed by an unauthorized person, they must immediately report the incident to the Area Registrar so swift action can be taken to secure the database.

7. Acknowledgment
By accepting access to the Area 15 Airtable database, you acknowledge that you have read, understand, and agree to strictly abide by these Data Privacy & Security Guidelines. You understand that protecting the privacy of your fellow members is your highest priority in this service position.