Lakemoor Community Club

Member Data Privacy and Confidentiality Policy

DRAFT — for review. Adoption date, notification timelines, and the open item in Section 5(b) require Board decision before final approval. *Additional notes in purple will not remain in policy.*

1. Purpose

This policy establishes standards for the collection, use, storage, and disclosure of member information by the Board of Directors, officers, committees, employees, contractors, and vendors of Lakemoor Community Club ("the Association"). It is intended to protect member privacy, support the Association's obligations under applicable Washington law, and provide a consistent, non-discretionary process for responding to data incidents. This policy is a standing governance document and applies prospectively to all data handling by the Association, not to any single past event.

Further, if there is a data breach, this policy will show that the organization attempted to protect data and shifts the responsibility for following policy to the individual in most cases.

2. Scope

This policy applies to every individual or entity who obtains Member Data through a role with the Association, including:

- Board members and officers Previous board members and officers *should* return or delete any data provided by the organization, rather than require discretion in perpetuity.
- Standing and advisory committee members
- The Association's management company and its personnel
- Independent contractors and vendors engaged by the Association
- Any other volunteer granted access to member records in the course of Association business

The newsletter and directory are NOT in scope, as these are publication neighbors agree to participate in. The focus is on data members must share to participate - think email for noticing, or financial account information.

3. Definitions

Member Data means any information the Association collects, maintains, or has access to regarding an individual member, including but not limited to name, mailing address, email address, phone number, lot or parcel identification, account and payment history, and correspondence submitted to the Association through the clerk or the management company.

Financial/Account Data means member ledger, dues, assessment, or payment information maintained by the Treasurer or the Association's management company.

Sensitive Personal Information means information beyond basic contact and account data — for example, information submitted in connection with a complaint, accommodation request, or dispute — that carries a heightened expectation of privacy.

4. Permitted Use of Member Data

Member Data is collected and maintained for Association governance purposes only — including legally required notices, official communications, billing, and recordkeeping. Member Data may not be used by any board member, committee member, contractor, or vendor for personal, political, commercial, or other purposes unrelated to their authorized Association role, and may not be shared with any third party without Board authorization.

Use of Member Data — including contact information — for unsolicited personal communication outside the recipient's authorized purpose is prohibited. This prohibition applies regardless of the sender's stated intent; a use that was not malicious can still violate this section.

5. Data Handling Standards

(a) Mass communications. Any communication sent to the full membership or any subset of members must be sent using blind carbon copy (BCC) or a distribution tool that does not expose recipient addresses to one another. Sending a group communication in a way that discloses member addresses to other recipients is a reportable data incident under Section 7, regardless of intent or the sender's role.

(b) Financial/Account Data access. Access to financial/account data is limited to the Treasurer, the Association's management company, and any officer or committee member whose access has been affirmatively authorized in writing by the Board for a defined purpose.

(c) Storage. Member data should be stored only in systems or files accessible to those with an authorized need, and should not be forwarded, copied, or stored in personal accounts except as required to complete an authorized Association task. Data stored in personal accounts is expected to be deleted or removed once the Association task is complete.

6. Contractors and Vendors

A contractor or vendor granted access to Member Data — including an email distribution list — for the purpose of performing Association work does not thereby acquire ownership of, or any independent right to use, that data. Data provided for a specific task may be used only for that task, and must be returned or deleted upon completion of the task, at the Board's request, or upon termination of the engagement. This requirement should be incorporated into future contractor and vendor agreements as a written term, not left as an unstated expectation.

7. Incident and Breach Notification

A “data incident” includes, without limitation: disclosure of Member Data to unauthorized recipients, use of Member Data outside its authorized purpose, or loss of control over Association records containing Member Data — regardless of whether the cause was intentional, accidental, or a technical error.

(a) Reporting. Any board member, officer, committee member, contractor, or vendor who becomes aware of a data incident must report it to the Board President and Secretary within [X] business days of becoming aware.

(b) Logging. The Board must record the incident in a written incident log, including the date, nature of the incident, data involved, number of members affected, and remedial action taken. This log is retained as an Association record independent of this policy.

(c) Member notification. Members whose data was involved in an incident must be notified in writing within [X] days of the Board's confirmation of the incident. The notification must describe what happened, what data was involved, and what steps are being taken.

(d) Independent of severity determination. The internal reporting, logging, and notification steps above apply regardless of the Board's assessment of severity or fault. Whether an incident meets the legal definition of a “breach” for purposes of any external reporting obligation is a separate legal determination and does not excuse or delay the internal steps in this section.

8. Non-Compliance

Violation of this policy by a board member, officer, or committee member may be referred to the Board for appropriate action, up to and including removal from the role, consistent with the Association's governing documents. Violation by a contractor or vendor may result in termination of the engagement.

9. Review

This policy will be reviewed by the Board no less than every two years, or promptly following any data incident, whichever occurs sooner.