

President's Report: Confidentiality and Data Privacy



January 2026

Prepared by CLFPD Board President Robin Lauric for the January 15th Crystal Lakes Fire Protection District Regular Board Meeting

I want to start by wishing everyone good health, prosperity, and much happiness (complete with some deep belly laughs) in the New Year.

A quick reminder of our collective responsibility to maintain the confidentiality of all District and Department records.

The Board and members of the Department are entrusted with sensitive information and are expected to handle it with the utmost discretion.

All members of the District are expected to exercise diligent care in safeguarding sensitive information. This includes, but not limited to personal medical details, phone numbers, physical addresses, lot and filing data, information obtained from property assessments or elections, and email addresses.

Email addresses, once collected, are classified as official District records, and their use or disclosure is strictly regulated. Collecting, sharing, or distributing email addresses without explicit approval from the Board or Chief is both inappropriate and, in most instances, unlawful. Any communication to property owners must be authorized and sent through official Department/District channels. Unauthorized sharing or use of emails not only breaches privacy but can expose individuals to risks such as spam, fraud, or harassment, violating their rights and eroding trust.

Communications within the District and Department should be conducted with the utmost responsibility, adhering to best practices such as utilizing blind carbon copy (bcc) when and refraining from sharing personal email addresses without explicit consent. These measures are essential to safeguard privacy and prevent the misuse of members' data.

The District and its members are subject to all relevant privacy regulations, and the Board acts as a steward to protect member data from misuse, such as the risks previously mentioned of spam, fraud, or harassment.

All members have a duty to promptly report any suspected or confirmed misuse of confidential information to the Chief or a member of the Board, ensuring the ongoing protection of our community's data and trust.

Board members have a fiduciary duty to protect member data and uphold privacy standards.