Technology Board Report

February 2026 - Sam Rigby

E-rate Internet - FY26

We are in the midst of the competitive bidding process for internet services starting 7/1/26. All bids are due by 2/18/26, at 11:00 PM. We have received one bid to date from Microcom, our current provider. Their proposed pricing remains competitive and very close to our existing costs.

Once all bids are received, we will evaluate them using the weighted criteria outlined in our RFP:

- Price per Bandwidth (Cost-Effectiveness of E-rate-Eligible Services) – 50 points
- Experience Serving Rural Alaska – 30 points
- Compliance with RFP Requirements – 20 points

Infrastructure Consolidation & Cost Optimization - We continue comprehensive reviews of our infrastructure and software systems to lower recurring costs without sacrificing functionality or service quality. These efforts support long-term budget stability while meeting educational needs.

AI Governance & Policy Development - As AI tools grow more common in education, LPSD is proactively developing policies and governance frameworks for responsible, secure use. We are:

- Creating a staff AI usage policy and acceptable use guidelines
- Building a technical governance framework for emerging technologies
- Ensuring full compliance with student data privacy laws (FERPA, COPPA)
- Carefully balancing innovation with security and ethical standards

These steps position us to safely adopt beneficial AI while protecting our students and staff.

Cybersecurity - Cybersecurity remains a top priority. Our district faces active threats to infrastructure and accounts every day. We are implementing advanced log monitoring and threat remediation tools to centralize visibility across all systems and align with key compliance and security standards.

Recent Phishing Incident (1/22/26) - A compromised email account from a known vendor was used to send targeted phishing emails to 10 LPSD staff members. Because the sender appeared legitimate, the messages evaded our automated filters and did not immediately alert recipients. One staff account was briefly accessed, but no data was removed and no further movement occurred within our network.

We responded immediately, revoked credentials, locked out the attacker, and conducted a full review of activity with no evidence of sensitive data exposure. This incident was contained thanks to several key safeguards:

- Our zero-trust approach, which limits every account to only the access needed for specific tasks and greatly reduces potential damage.
- Multi-factor authentication (MFA), which blocked access attempts on at least one other compromised account.
- Ongoing staff training, which remains essential since human factors are often the weakest link in security.

No reporting was required under Alaska regulations, as no data was compromised.