Young Elementary School District

District had higher administrative costs than peer districts and spent unauthorized monies on its community preschool program, and its lack of compliance with important standards and requirements put public monies and sensitive information at risk

Audit purpose

To assess the District's efficiency and effectiveness in 4 operational areas—administration, plant operations and maintenance, food service, and transportation—and its compliance with certain State requirements.

Key findings

- District spent over $264,000 more on administration than peer districts in fiscal year 2020 primarily because of additional administrative staff and higher salaries, 1-time payouts to individuals who separated employment, and associated legal fees.

- District spent $21,600 of unauthorized monies on its community preschool program in fiscal year 2021.

- District did not always use prenumbered receipts or ensure all cash collected was deposited in a timely manner, possibly resulting in lost cash and increasing risk of errors or fraud.

- District allowed excessive access to its sensitive computerized data and operated with other IT deficiencies, which increased the risk of unauthorized access, errors, fraud, and data loss.

Key recommendations

The District should:

- Monitor its administrative spending and identify and implement ways to reduce it, including by specifically assessing its administrative staffing and salary levels.

- Determine whether it should continue offering its community preschool program and, if it does, charge fees or student tuition rates and/or obtain grants or donations that cover the costs of operating the program consistent with statute and Arizona Attorney General opinion No. I82-136.

- Help ensure staff members comply with USFR requirements to safeguard cash.

- Limit its user access to those accounting system operations needed to perform job duties, and develop and implement a new process to assign new users appropriate access.

- Immediately remove terminated employees' network accounts, and develop and implement a process to ensure that terminated employees have their access promptly removed.

- Develop and implement an IT contingency plan and test the plan at least annually.