Office of Missouri State Auditor

Nicole Galloway, CPA

Orchard Farm R-V School District

Student Data Governance

Report No. 2016-089
September 2016

auditor.mo.gov

September 2016

Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the Cyber Aware School Audit of the Orchard Farm R-V School District

Background

The Orchard Farm R-V School District's Student Data Governance Audit was completed as part of the Cyber Aware School Audits Initiative. These audits are designed to assess the effectiveness of privacy and security controls with a focus on identifying practices to improve the security of information school districts have on students and their families. The district uses a student information system (SIS) to maintain student data and to track and monitor academic progress. The SIS maintains private and confidential data, such as assessment test scores and other sensitive data. Additional systems and applications that maintain data are used for administrative functions and to enhance student productivity and classroom collaboration. The district relies extensively on computerized systems to support its educational and mission-related operations and on information security controls to protect the sensitive data residing on those systems. Auditors identified areas where improvements are needed but also found the district has developed certain controls to establish a safe environment for using technology, including promoting online safety, security, and confidentiality.

Data Governance

The district has not completed establishing a comprehensive data governance program, a critical task for any educational organization. A comprehensive program is necessary to ensure the confidentiality, integrity, availability, and quality of data. Without a formal program, the district cannot ensure that personally identifiable information (PII) is adequately protected and safe from unauthorized access, misuse, or inadvertent disclosure.

Review of User Access

The district does not perform periodic reviews of users' access to data to ensure access remains appropriate and aligned with job duties. As users' work assignments and job responsibilities change, access rights to systems may be added, changed, or removed. Over time, users can accumulate access rights that are no longer necessary, increasing the risk of inappropriate access to data.

Security Controls

The district has not implemented or documented policies and procedures for certain security controls, leaving district technology assets, including PII, at risk of inappropriate access, use, and disclosure. The district has not documented policies and procedures to identify the types of security events to be logged and monitored. The district has not documented policies and procedures for certain security controls. Without documented and approved policies and procedures, management may not have assurance that control activities are appropriate and properly applied.

Continuity Planning

The district has not completed or formally tested its continuity plan. District personnel created a continuity plan in 2013; held discussions to add key contacts and vendors to the plan; and updated the plan in July 2016, indicating the district has made progress. However, the plan needs to be completed and formally tested. Without a tested and functional continuity plan, management has limited assurance the organization's business functions and computer processing can be sustained during or promptly resumed after a disruptive incident.

Vendor Controls

The district has not established a process for ensuring software acquired or outsourced from information technology vendors complies with data security principles, and the district's contract for a key system does not fully define expectations over securing and accessing district data. Data maintained by the system is hosted locally by the district. However, data is also routinely backed up to the vendor site. Without an effective process for monitoring and managing risk of software acquisition or outsourcing, and without fully defining expectations over district data, the district has less assurance in a vendor's ability to deliver services effectively, securely, and reliably and to ensure that services meet current and future data privacy and security needs.

Because of the nature of this report, no overall rating is provided.

All reports are available on our Web site: auditor.mo.gov

Orchard Farm R-V School District Student Data Governance
Table of Contents

NICOLE GALLOWAY, CPA
Missouri State Auditor

To the Board of Education
Orchard Farm R-V School District

Due to increasing concerns for protecting the security and privacy of information schools maintain on students and the continued emergence of cyber threats, we have audited the Orchard Farm R-V School District's student data governance program in fulfillment of our duties under Chapter 29, RSMo. This audit was conducted as part of the State Auditor's Cyber Aware School Audits Initiative and focused on evaluating the effectiveness of the data governance program, including identifying cybersecurity safeguards and privacy controls that help schools improve the security of student data.

The objectives of our audit were to:

1. Evaluate the effectiveness of privacy plans and controls for safeguarding personally identifiable information.

2. Evaluate the effectiveness of information security controls for protecting the confidentiality, integrity, and availability of significant systems and information technology resources.

3. Evaluate compliance with certain legal provisions.

We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform our audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides such a basis.

For the areas audited, we identified (1) the need to fully establish certain privacy plans and controls, (2) the need to fully establish certain information security controls for protecting the confidentiality, integrity, and availability of significant systems and information technology resources, and (3) no significant noncompliance with legal provisions.

The accompanying Management Advisory Report presents our findings arising from our audit of the Orchard Farm R-V School District's student data governance program.

Nicole R. Galloway, CPA
State Auditor

The following auditors participated in the preparation of this report:

Deputy State Auditor:	Keriann Wright, MBA, CPA
Director of Audits:	Douglas J. Porting, CPA, CFE
Audit Manager:	Lori Melton, M.Acct., CPA
In-Charge Auditor:	Alex R. Prenger, M.S.Acct., CPA
Audit Staff:	Michelle Johnson

Orchard Farm R-V School District Student Data Governance Introduction

Background

The Orchard Farm R-V School District Student Data Governance Audit was completed as part of the Cyber Aware School Audits Initiative. These audits are designed to assess the effectiveness of privacy and security controls with a focus on identifying practices to improve the security of information school districts have on students and their families.

The district uses a student information system (SIS) to maintain student data and to track and monitor academic progress. The SIS maintains private and confidential data, such as student names and addresses, assessment test scores, and other sensitive data. The district uploads various student data maintained in the SIS to the Department of Elementary and Secondary Education (DESE), Missouri Student Information System (MOSIS) Data Collection component periodically throughout the year. The MOSIS Data Collection component is used to collect student-level data from school districts for processing and reporting. Data submitted by the district includes elements such as enrollment and attendance, demographics, performance information, and college and career data used for evaluating the success and achievements of students. The district also uses a financial accounting system and a network management system for administering user access to various district resources. Other systems and applications are used for administrative functions and to enhance student productivity and classroom collaboration.

Cyber threats continue to emerge and evolve

As connectivity of business activity increases and organizations become increasingly dependent on technology, including computerized systems and electronic data, no school district is exempt from cyber threats, vulnerabilities, and privacy exposures. As a result, it is important to view information security and privacy as a business issue rather than strictly an information technology issue. Security threats, vulnerabilities, and privacy exposures challenge every organization, creating data protection and privacy risks that must be understood, addressed, and managed.

The National Institute of Standards and Technology (NIST) defines cybersecurity as the process of protecting information by preventing, detecting, and responding to attacks[1] while ISACA states cybersecurity encompasses all that protects enterprises and individuals from intentional attacks, breaches and incidents as well as the consequences.[2] Cybersecurity should be aligned with all other aspects of information security, including governance, management, and assurance. The state of being secure requires

[1] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1, February 2014, is available at <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>.

[2] ISACA Cybersecurity Nexus, Transforming Cybersecurity, 2013.

maintenance and continuous improvement to meet the needs of stakeholders and the demands of emerging cyber threats.

In the 2015 High-Risk Series[3] update, the Government Accountability Office (GAO) expanded the scope of the information security high-risk area to include protecting the privacy of personally identifiable information (PII).[4] The GAO expanded this risk area due to the challenges of ensuring the privacy of PII created by advances in technology. Technology advances, such as lower data storage costs and increasing interconnectivity, have allowed both government and private sector agencies to collect and process extensive amounts of PII more effectively. Risks to PII can originate from unintentional and intentional threats. These risks include insider threats from careless, disgruntled, or improperly trained employees and contractors; the ease of obtaining and using hacking tools; and the emergence of more destructive attacks and data thefts.

Technology advances, combined with the increasing sophistication of individuals or groups with malicious intent, have increased the risk of PII being compromised and exposed. Correspondingly, the number of reported security incidents involving PII in both the private and public sectors has increased dramatically in recent years. At the same time, school districts are increasingly reliant on technology and information sharing to interact with students and parents and to deliver essential educational services. As a result, the need to protect information, including PII, against cyber threats is increasingly important.

The Privacy Rights Clearinghouse[5] recorded breaches at kindergarten through grade 12 (K-12) educational institutions/school districts in the United States occurring during 2005 through 2015, potentially disclosing over 580,000 records of personal information.[6] These breaches include only

[3] Report GAO-15-290, Report to Congressional Committees, High-Risk Series An Update, February 2015, is available at <http://www.gao.gov/assets/670/668415.pdf>.

[4] According to the Family Educational Rights and Privacy Act (FERPA), personally identifiable information (PII) includes, but is not limited to (a) the student's name; (b) the name of the student's parent or other family members; (c) the address of the student or student's family; (d) a personal identifier, such as the student's social security number, student number, or biometric record; (e) other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; and (f) other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student.

[5] The Privacy Rights Clearinghouse is a nonprofit corporation whose mission is to engage, educate, and empower individuals to protect their privacy by raising awareness of how technology affects personal privacy.

[6] Privacy Rights Clearinghouse, Chronology of Data Breaches, is available at <http://www.privacyrights.org/data-breach>. We downloaded a file containing all breaches and filtered the results to include only data breaches occurring at K-12 educational institutions.

those made public and the data reflects three data breach incidents at Missouri public school districts.

Data governance

According to the U.S. Department of Education, Privacy Technical Assistance Center (PTAC),[7] data governance is an organizational approach to data and information management that is formalized as a set of policies and procedures encompassing the full life cycle of data, from acquisition to use to disposal. It includes establishing policies, procedures, and standards regarding data security and privacy protection, data inventories, content and records management, data quality control, data access, and data sharing and dissemination. Establishing a comprehensive data governance program helps ensure confidentiality, integrity, and availability of data and information by reducing data security risks due to unauthorized access or misuse of data.

Security and privacy controls

According to accepted standards, security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of a system and its information. Confidentiality refers to preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information. Integrity relates to guarding against improper information modification or destruction, and availability ensures timely and reliable access to and use of information. Effective privacy controls depend on the safeguards employed within the information system that is processing, storing, and transmitting PII and the environment in which the system operates. Organizations cannot have effective privacy without a basic foundation of information security. Without proper safeguards and controls, information systems and confidential data are vulnerable to individuals with malicious intentions who can use access to obtain sensitive data or disrupt operations.

Laws and regulations

Various federal and state laws and regulations pertain to the protection of sensitive student data, including the Family Educational Rights and Privacy Act (FERPA), the Individuals with Disabilities Education Act (IDEA), and the Protection of Pupil Rights Amendment (PPRA). Additionally, Section 161.096, RSMo, requires the State Board of Education to promulgate a rule regarding "student data accessibility, transparency, and accountability."[8]

[7] U.S. Department of Education, Privacy Technical Assistance Center, Data Governance Checklist, is available at <http://ptac.ed.gov/sites/default/files/Data%20Governance%20Checklist%20%281%29.pdf>.

[8] 5 CSR Section 20-700.100

Controls established

The district has an important responsibility for maintaining the privacy of student data and for implementing and maintaining information security controls. The district relies extensively on computerized systems to support its educational and mission-related operations and on information security controls to protect the sensitive data residing on those systems. While we found areas where improvements are needed, as discussed in the Management Advisory Report, we also found the district has established:

- A technology usage policy to facilitate access to district technology and to create a safe environment for using the technology, including promoting online safety, security, and confidentiality.
- A comprehensive privacy and security awareness training program to assure a complete understanding of the importance of privacy and security by all personnel.
- Security controls regarding logon banners, concurrent use, and the physical protection of technology resources, as well as formal appointment of a district security administrator.
- Documented procedures for incident response and data breach response.
- Policies and procedures, including applicable parent/student forms, required to be in compliance with the FERPA data disclosure and usage provisions.
- The controls and processes required to be in compliance with the Children's Internet Protection Act (CIPA).
- Certain controls designed to help ensure the privacy of data and to help ensure the confidentiality, integrity, and availability of significant systems and data maintained on those systems.

Cyber threats will continue to challenge operational resilience and business continuity preparedness. School districts can reduce the risks of breaches by remaining aware of emerging cyber threats and consider the potential impact to operational resilience.

Scope and Methodology

The scope of our audit included the Orchard Farm R-V School District's approach to data governance, including information security, privacy, and other relevant internal controls; policies and procedures; and other management functions and compliance issues in place.

Our methodology included reviewing written policies and procedures, and interviewing various district personnel. We obtained an understanding of the data governance approach and applicable controls that are significant within the context of the audit objectives and assessed whether such controls have been properly designed and placed in operation. We tested certain of those controls to obtain evidence regarding the effectiveness of their design and operation. We also obtained an understanding of legal provisions that are significant within the context of the audit objectives, and we assessed the risk that illegal acts, including fraud, and violation of contract or other legal provisions could occur. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to those provisions.

We obtained a list of district employees as of June 2016 from the district's accounting system. We matched these records to the user account records from the district's student information system, financial accounting system, and network management system to determine if any terminated employees had active accounts. We also matched these records to users of the DESE statewide data collection systems. Although we used computer-processed data from these systems for our audit work, we did not rely on the results of any processes performed by these systems in arriving at our conclusions. Our conclusions were based on our review of the issues specific to the audit objectives.

We based our evaluation on accepted state, federal, and international standards; policies and procedures; and best practices related to information technology security and privacy controls from the following sources:

- National Institute of Standards and Technology (NIST)
- Government Accountability Office (GAO)
- ISACA (previously known as the Information Systems Audit and Control Association)
- U.S. Department of Education, Privacy Technical Assistance Center (PTAC)[9]

[9] According to its web site, the U.S. Department of Education established the PTAC as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems. The PTAC provides information and guidance on privacy, confidentiality, and security practices through a variety of resources. PTAC information is available at <http://nces.ed.gov/programs/ptac>.

1. Data Governance

The district has not completed establishing a comprehensive data governance program. As a result, there is less assurance the data management and protection procedures in place are effective in reducing data privacy and security risks due to unauthorized access or misuse of data.

According to the U.S. Department of Education, Privacy Technical Assistance Center (PTAC), data governance is necessary to ensure the confidentiality, integrity, availability, and quality of data. Establishing a data governance program is a critical task for any educational organization. An effective program requires establishing decision-making authority, defining policies and practices for the protection of sensitive data, identifying and gaining support of stakeholders, implementing the program, and monitoring its success. By clearly establishing policies, standard procedures, responsibilities, and controls for data activities, a data governance program helps to ensure that information is collected, maintained, used, and disseminated in a manner that protects privacy, confidentiality, and security, while allowing educational organizations to meet their missions.

During our review of the district's data governance approach, we found improvements are needed in the following component areas:

- Responsibility for data management
- Data stewardship
- Inventory of classified data
- Source and content of data
- Archival and/or destruction of data at the end of its lifecycle

The district has not formally assigned responsibility for management of the district's data. Assigning appropriate levels of authority to data stewards and proactively defining the scope and limitations of that authority is a prerequisite to successful data management.

The district has not developed a formalized data stewardship plan documenting policies and procedures to protect student data. Adopting and enforcing clear policies and procedures in a written data stewardship plan is necessary to ensure everyone in the organization understands the importance of data quality and security, and staff are motivated and empowered to implement data governance.

The district does not maintain an inventory of data files. Conducting an inventory of all data that require protection is a critical step for data security projects. Maintaining an up-to-date inventory of all sensitive records and data systems, including those used to store and process data, enables the organization to target its data security and management efforts.

The district has not formally identified the source and content of elements within the data files maintained by the district. Closely managing data content, including identifying the purposes for which data are collected, is necessary to justify the collection of sensitive data, optimize data management processes, and ensure compliance with federal, state, and local regulations.

The district has not adopted a formal policy regarding the archival or destruction of data at the end of its lifecycle. While some data may need to be maintained indefinitely according to various laws and regulations, other data may become unnecessary or irrelevant when a student graduates or otherwise leaves the district, and can be destroyed when no longer needed. Planning for data archival or destruction is an integral part of a high quality data governance program, according to the U.S. Department of Education, PTAC. Data destruction is the process of removing information in a way that renders it unreadable (for paper records) or irretrievable (for digital records). Establishing policies and procedures governing the archival or destruction of data allows an organization to more efficiently and safely protect its data and is a critical component of an effective data governance program.

Without a formal data governance program, the district cannot ensure that personally identifiable information (PII) maintained by the district is adequately protected and safe from unauthorized access, misuse, or inadvertent disclosure.

Recommendation

The district should continue to establish and implement a formal data governance program encompassing the full life cycle of data, from acquisition to use to disposal.

Auditee's Response

The district concurs with the recommendation and will develop and implement a formal data governance program encompassing the full life cycle of data by March 2017.

2. Review of User Access

The district does not perform periodic reviews of users' access to data to ensure access remains appropriate and aligned with job duties.

As users' work assignments and job responsibilities change, access rights to systems may be added, changed, or removed. Over time, users can accumulate access rights that are no longer necessary, increasing the risk of inappropriate access to data.

Without periodically reviewing user access rights, there is an increased risk that unauthorized alterations of the rights will go undetected or that access rights may not be aligned with current job duties.

Recommendation

The district should periodically review user access to data and other information resources to ensure access rights remain appropriate and are commensurate with job duties and responsibilities.

Auditee's Response

The district concurs with the recommendation and will further revise the district's procedures to ensure access rights remain appropriate and are commensurate with job duties and responsibilities by March 2017.

3. Security Controls

The district has not implemented or documented policies and procedures for certain security controls, leaving district technology assets, including PII, at risk of inappropriate access, use, and disclosure.

Logical security is the use of computer hardware and software to prevent or detect unauthorized access to systems, including the data therein. Logical security most often takes the form of user accounts and passwords, but also includes location and network based controls and security hardware, such as firewalls.

3.1 Security logs

The district has not documented policies and procedures to identify the types of security events to be logged and monitored. As a result, there is less assurance that detected and logged security incidents are properly investigated and resolved.

The internal security policies within the district's network management system log thousands of entries each day. A majority of these entries, such as notification of successful login by system users, are of minimal use for security purposes. According to district staff, the network management system default logging settings are used. Because the district has not customized these settings regarding which events are logged, the security logs are voluminous and cannot effectively be monitored for unusual or suspicious activity.

The district should establish relevant criteria and identify significant system events that should be logged. At a minimum, all such significant events, including access to and modification of sensitive or critical system resources, should be logged. Also, logging should include appropriate information to facilitate monitoring of such significant system events.

Without an effective method to identify, log, and monitor significant security-relevant events, the district is at increased risk that unauthorized or inappropriate system activity may not be detected.

3.2 Documentation of security controls

The district has not documented policies and procedures for certain security controls.

According to the GAO standards for internal control, control activities are an integral part of an organization's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives and helps ensure that actions are taken to reasonably address risks. The following control activities, including policies and procedures, have not been fully documented:

- Resetting lost or compromised passwords.
- Documentation of procedures for establishing user access to data and other resources for certain systems.
- Policies regarding which security groups users may be assigned to, along with the access rights granted each group for certain systems.
- Policies describing who may be granted privileged access to district systems.

According to accepted standards, documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently.

Without documented and approved policies and procedures, management may not have assurance that control activities are appropriate and properly applied.

Recommendations

The district:

3.1 Establish and document criteria for identifying which security events should be written to audit logs, monitored and investigated as security incidents.

3.2 Fully document and regularly review security policies and procedures.

Auditee's Response

3.1 The district concurs and will review and revise documentation for identifying which security events should be written to audit logs and monitored and investigated as security incidents by March 2017.

3.2 The district concurs with the recommendation and will fully document and review security policies and procedures by March 2017.

4. Continuity Planning

The district has not completed or formally tested its continuity plan.

Elements of a continuity plan the district has not documented include:

- Priorities and procedures for the restoration of critical systems and data.
- Identification of persons responsible for restoration of specific systems and data.

According to accepted standards, a continuity plan or suite of related plans should be developed for restoring critical business functions and applications. The plans should include arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed.

Additionally, testing continuity plans is essential to determining whether the plans will function as intended in an emergency situation. The most useful scenarios involve simulating a disaster situation to test overall service continuity. Such an event would include testing whether the alternative data processing site will function as intended and whether critical computer data and programs recovered from off-site storage are accessible and current. Moreover, tests will assess how well employees have been trained to carry out their roles and responsibilities in a disaster situation. Any testing of continuity plans is likely to identify weaknesses in the plan, and it is important that the plan and related supporting activities, such as training, be revised to address these weaknesses. Otherwise, the benefits of the testing will be mostly lost.

District personnel created a continuity plan in 2013; held discussions to add key contacts and vendors to the plan; and updated the plan in July 2016, indicating the district has made progress. However, the plan needs to be completed and formally tested. Without a tested and functional continuity plan, management has limited assurance the organization's business functions and computer processing can be sustained during or promptly resumed after a disruptive incident.

Recommendation

The district should continue developing a comprehensive continuity plan and formally assign responsibilities for implementation and maintenance of the plan to appropriate personnel. Once established, ensure the plan is tested on a periodic basis.

Auditee's Response

The district concurs and will continue developing a comprehensive continuity plan. The district will also formally assign the responsibilities for implementation and maintenance to the appropriate personnel. The district will also establish a routine for testing the continuity plan by March 2017.

5. Vendor Controls

The district has not fully established vendor monitoring controls. Additionally, the district's contract for a key system does not fully define security and privacy expectations over district data.

5.1 Vendor monitoring

The district has not established a process for ensuring software acquired or outsourced from information technology vendors complies with data security principles.

The district utilizes software products from a number of vendors to manage financial information, human resources data, student data, and other information. Generally, the district pays an annual licensing/maintenance fee for these products. Depending on the arrangement, some products are installed on district-owned equipment and maintained by district personnel (with additional support from the vendor), while others are hosted and maintained directly by the vendor. In this case, district personnel access the system remotely, typically via a secure website.

We reviewed contracts for several systems or software products used by the district. Although the specific language varied, each contract had a clause stating the vendor would provide appropriate security functionality for the district. However, district staff indicated they had not asked any vendors to provide documentation that their product's security functionality met generally accepted industry standards.

Accepted standards require organizations to periodically review the overall performance of vendors, compliance to contract requirements, and value for money, and address identified issues. Without an effective process for monitoring and managing risk of software acquisition or outsourcing, the district has less assurance in a vendor's ability to deliver services effectively, securely, and reliably and to ensure that services meet current and future data privacy and security needs.

5.2 Vendor contract

The district's contract for a key system does not fully define expectations over securing and accessing district data. Data maintained by the system is hosted locally by the district. However, data is also routinely backed up to the vendor site.

Accepted standards require organizations to manage, maintain and monitor contracts and service delivery. The U.S. Department of Education, PTAC provides best practices for organizations entering into written agreements. These best practices include stating ownership of PII; agreeing on limitations on use of PII, including restrictions on marketing, advertising and data mining purposes; and maintaining data in a secure manner by applying appropriate technical, physical, and administrative safeguards to properly protect PII. These also include setting terms for data destruction, identifying penalties for inappropriate disclosure; and defining terms for conflict resolution.

Without fully defining expectations over district data, the district cannot ensure the security and privacy of its data, and may be unable to rely on enforceable contractual provisions in the event of a vendor dispute or noncompliance.

Recommendations

The district:

5.1 Develop procedures to formally monitor information technology vendors to ensure the district's data is properly protected and the vendor acts in accordance with contract terms.

5.2 Improve the existing contract with the vendor defining expectations over securing and accessing district data.

Auditee's Response

5.1 The district will develop a formal plan to monitor vendor contractual agreements by March 2017.

5.2 The district will develop a formal rubric for contracts with outside vendors that have access to district data and will work with vendors using this rubric to improve existing contracts to improve expectations over securing and accessing district data by March 2017.

Orchard Farm R-V School District Student Data Governance Organization and Statistical Information

The Orchard Farm R-V School District is located in St. Charles County.

The district operates a high school (grades 9-12), a middle school (grades 6-8), two elementary schools (grades 1-5), and one preschool. An early learning center opened in August 2016. Enrollment (preK-12) was 1,850 for the 2015-2016 school year. The district employed 380 full- and part-time employees at June 1, 2016.

School Board and Key Personnel

An elected school board serves as the policy-making body for the district's operations. The board's seven members serve 3-year terms without compensation. Members of the board at June 1, 2016 were:

Nancy Goeke, President
Darren Grunwaldt, Vice President
Nathan Dunkmann, Treasurer
Casey Otto, Secretary
Kenneth Biermann, Member
Steven Stopke, Member
Sara Vacek, Member

Dr. Tom Muzzey serves as District Superintendent. Dr. Wade Steinhoff is the Assistant Superintendent, and Bill Niemeyer is the Chief Technology Officer.