



# **Rowland Unified School District**

## **Technology Review**

June 4, 2008

Joel D. Montero  
Chief Executive Officer





June 4, 2008

Maria Ott, Ph.D., Superintendent  
Rowland Unified School District  
1830 S. Nogales Street  
Rowland Heights, CA 91748

Dear Superintendent Ott,

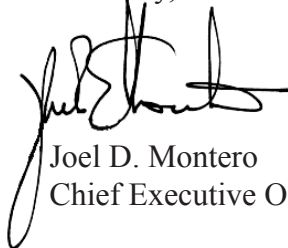
In May 2007, the Rowland Unified School District and the Fiscal Crisis and Management Assistance Team (FCMAT) entered into a study agreement to provide a review of the district's technology services. Specifically, the agreement asked FCMAT to perform the following:

1. Assess the organization and operations of the district's technology services department and make recommendations for improvement.
2. Conduct a review of the district's instructional implementation of technology and make recommendations for improvement.
3. Conduct a review of the district's administrative technology implementation and make recommendations for improvement.
4. Conduct a computer network security review and recommend improvements to harden network security precautions and improve network performance.

The attached final report contains the study team's findings and recommendations.

We appreciate the opportunity to serve you and we extend our thanks to all the staff of the Rowland Unified School District.

Sincerely,



Joel D. Montero  
Chief Executive Officer

FCMAT

Joel D. Montero, Chief Executive Officer

1300 17<sup>th</sup> Street - CITY CENTRE, Bakersfield, CA 93301-4533 • Telephone 661-636-4611 • Fax 661-636-4647  
422 Petaluma Blvd North, Suite. C, Petaluma, CA 94952 • Telephone: 707-775-2850 • Fax: 707-775-2854 • [www.fcmat.org](http://www.fcmat.org)  
Administrative Agent: Larry E. Reider - Office of Kern County Superintendent of Schools



Table of Contents

Foreword .....iii

Introduction ..... I

*Background* ..... 1

*Study Guidelines* ..... 2

*Study Team* ..... 2

Executive Summary ..... 3

Findings and Recommendations ..... 5

*Organization and Operations* ..... 5

*Policies* ..... 15

*Planning and Standards* ..... 17

*Instructional Technology* ..... 21

*Administrative Technology* ..... 23

*Network and Security* ..... 25

Appendices ..... 31



# Foreword

## FCMAT Background

The Fiscal Crisis and Management Assistance Team (FCMAT) was created by legislation in accordance with Assembly Bill 1200 in 1992 as a service to assist local educational agencies in complying with fiscal accountability standards.

AB 1200 was established from a need to ensure that local educational agencies throughout California were adequately prepared to meet and sustain their financial obligations. AB 1200 is also a statewide plan for county offices of education and school districts to work together on a local level to improve fiscal procedures and accountability standards. The legislation expanded the role of the county office in monitoring school districts under certain fiscal constraints to ensure these districts could meet their financial commitments on a multiyear basis. AB 2756 provides specific responsibilities to FCMAT with regard to districts that have received emergency state loans. These include comprehensive assessments in five major operational areas and periodic reports that identify the district's progress on the improvement plans.

Since 1992, FCMAT has been engaged to perform more than 600 reviews for local educational agencies, including school districts, county offices of education, charter schools and community colleges. Services range from fiscal crisis intervention to management review and assistance. FCMAT also provides professional development training. The Kern County Superintendent of Schools is the administrative agent for FCMAT. The agency is guided under the leadership of Joel D. Montero, Chief Executive Officer, with funding derived through appropriations in the state budget and a modest fee schedule for charges to requesting agencies.

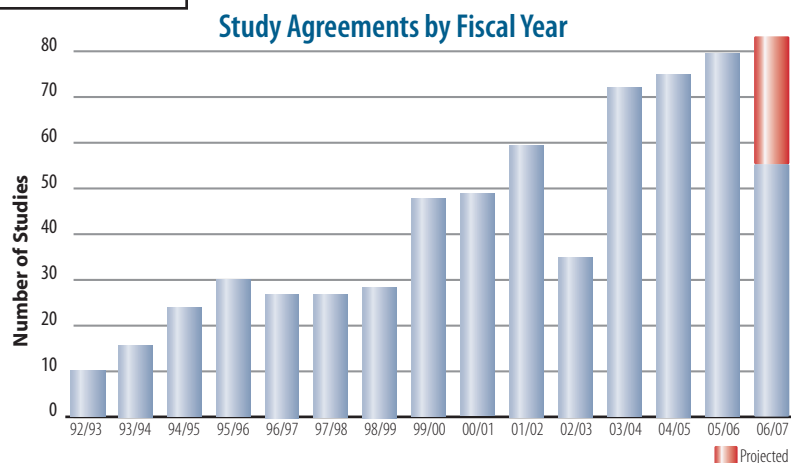
**Total Number of Studies..... 637**

**Total Number of Districts in CA ..... 982**

- Management Assistance..... 603 (94.66%)
- Fiscal Crisis/Emergency ..... 34 (5.34%)

Note: Some districts had multiple studies.

- Districts (7) that have received emergency loans from the state.  
(Rev. 4/3/07)







# Introduction

## *Background*

Located 40 miles east of Los Angeles, the Rowland Unified School District serves 18,000 students and at 23 elementary and secondary schools and approximately 5,000 adults through adult and community education programs. The district has distinguished itself by earning more school and state level honors than any other school district in the region.

In May 2007, the district and the Fiscal Crisis and Management Assistance Team entered into a study agreement for a review of the district's technology services. Specifically, the agreement asked FCMAT to:

1. Assess the organization and operations of the district's technology services department and make recommendations for improvement.
2. Conduct a review of the district's instructional implementation of technology and make recommendations for improvement.
3. Conduct a review of the district's administrative technology implementation and make recommendations for improvement.
4. Conduct a computer network security review and recommend improvements to harden network security precautions and improve network performance.

The district has developed a variety of innovative academic programs that contribute to improved student achievement. However, district board members have expressed a perception that the district could do more with respect to instructional technology and have conveyed an increasing interest in using technology to enhance teaching and improve student performance.

For many years the selection, procurement and implementation of technology have been decentralized, with sites planning for and purchasing technology assets independently. As a result, disparate, incompatible systems have been implemented; the advantages of collective purchasing power have been lost; and the lack of standards has created a significant support problem for technology support services staff.

Seeking to improve student performance, district administrators have discussed alternatives to improve the effectiveness of technology support and service delivery with increasingly limited resources.

### *Study Guidelines*

A FCMAT study team visited the district on May 22, 2007 to conduct interviews, collect data and review documents. This report is the result of those activities and is divided into the following sections:

- I. Executive Summary
- II. Organization and Operations
- III. Policies
- IV. Planning and Standards
- V. Instructional Technology
- VI. Administrative Technology
- VII. Network and Security

### *Study Team*

Andrew Prestage  
Management Analyst  
FCMAT  
Bakersfield, CA

Bradley White\*  
Senior Network Engineer  
Lightspeed Systems  
Bakersfield, CA

Warren Williams\*  
Assistant Superintendent  
Grossmont Union High School District  
La Mesa, CA

John Lotze  
Public Information Specialist  
FCMAT  
Bakersfield, CA

\*As members of this study team, these consultants were not representing their respective employers but were working solely as independent contractors for FCMAT.

## Executive Summary

The Rowland Unified School District is in a good position to create a sustainable technology program that will benefit students and teachers while performing the administrative functions of the district.

Currently, responsibility for technology support services is spread across two departments reporting within two separate divisions. No single individual in the district is charged with responsibility for all aspects of administrative and instructional technology. This fragmented organizational structure has blurred lines of responsibility for technology support. Many staff shared a perception that no one in the district has a grasp of how technology should be integrated with instruction. Consolidation of the departments into a single technology support services department would eliminate redundancies and provide opportunities for increased efficiency and effectiveness.

The current method used to assign technology support staff to school sites for technical repairs or upgrades is ineffective. Site administrators expressed a desire to know when support staff will be at their sites. Communications within and between departments that provide technology support services is insufficient. Improved communication, scheduling and coordination are needed.

Many obsolete computers are still in use but are not capable of running the latest operating systems and applications. The district should develop and implement a computer replacement strategy.

The district's student information system (SIS) is not backed up using standard, automated backup procedures. A plan to perform daily tape backups of the district's student information system should be developed immediately. The district's SIS data is at risk until a tape backup system can be implemented.

The district lacks a variety of policies and standards related to equipment replacement, disposal, and donation. Many district staff members have never signed an acceptable use policy (AUP) that defines acceptable and unacceptable use of district network resources such as Internet and e-mail. The district should develop and implement these policies and standards, including an AUP.

The district has had difficulty enforcing technology standardization across all sites. This has increased the level of difficulty and complexity associated with providing technology support services, and creates additional support costs. Enforced standards and standardization of equipment are needed to simplify technology support and increase efficiency.

The district's director of technology has the complex task of maintaining the district's E-Rate applications and documentation. The district should consider contracting with an experienced E-rate consultant for assistance completing applications and meeting deadlines.

The district's technology plan was recently updated by a limited number of staff without input from a wide variety of stakeholders. The plan will need to be developed anew with input from the extended educational community.

The district's network lacks network documentation. In addition, student and academic network traffic is not separated from administrative network traffic, creating a risk that any network user may access private information. The district should create separate logical networks for these two types of data.

Many network elements use the equipment vendor's default authentication settings, and others do not require passwords and user names to access, or allow access using default and commonly known passwords or settings. System logs and time stamps based on a common, synchronized network time are also lacking. Most of the district's network uses globally routable IP address space, a practice which is discouraged because other more secure address space has become available. The district should change network element default settings; require passwords; limit access to network elements through IP address access lists and other means; implement system logs and common time stamps using a network time protocol server; and configure the network to use non-globally routable IP address space to eliminate the risk of exposure to the global internet.

# Findings and Recommendations

## *Organization and Operations*

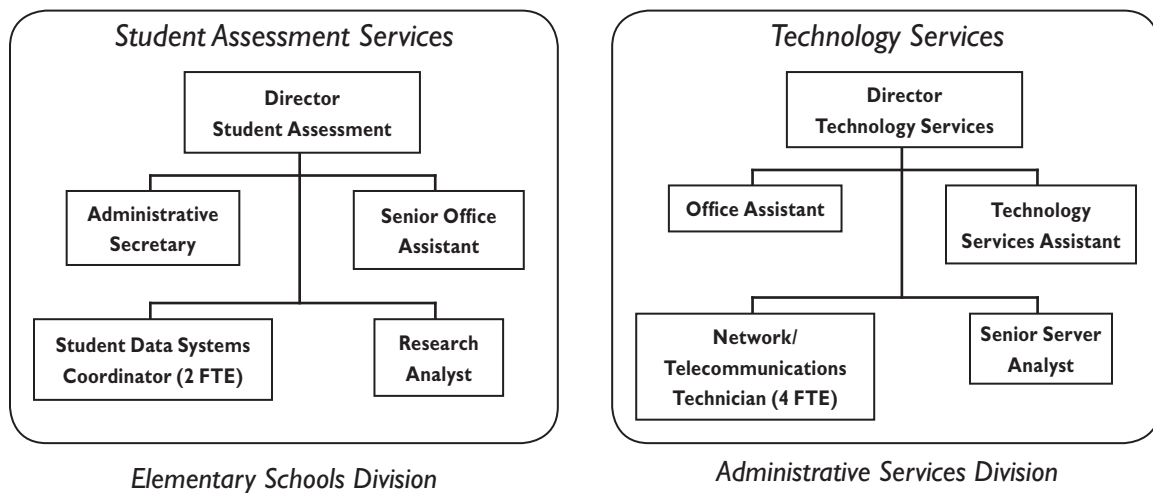
### *Organization*

Two separate departments within two separate divisions provide the district's technology support services and are responsible for delivering educational technology, information technology and network services support. No single individual in the district has responsibility for all aspects of administrative and instructional technology. This fragmented organizational structure has blurred lines of responsibility for support and has made it difficult for staff members to work cohesively with technology support staff members in other departments to improve technology service delivery.

Many staff indicated that there is no one who understands the global technology needs of the district or who is responsible for working with teachers to pursue instructional technology initiatives. Instructional staff expressed frustration that there is no one at the district level who has been assigned to plan how technology should be integrated with instruction. The research analyst position and standardized testing functions do not reside within the technology services department.

Consolidation of the technology services provided by the two independent departments would provide the district with an opportunity to eliminate redundancy while improving service delivery.

Staffing for technology services delivery has not grown in proportion with the increased demand for administrative and instructional systems and attendant computer infrastructure. The district's technology support function lacks sufficient personnel to effectively manage the district's technology resources. One reason for the staffing limitations within the technology services department is a lack of information at the cabinet level on issues related to technology. The technology services director is not a member of the cabinet and therefore is not present during discussions of technology issues. The current organizational structure of each department is depicted on the following page.



Personnel compensation associated with each department is indicated below.

**Student Assessment Services:**

Director, Student Assessment	1 FTE	
Student Data Systems Coordinator	2 FTE	
Research Analyst	1 FTE	
Senior Office Assistant	1 FTE	
Administrative Secretary	1 FTE	
Subtotal	6 FTE	\$337,730

**Technology Services:**

Director, Technology Services	1 FTE	
Network/Telecommunications Tech	4 FTE	
Senior Server Analyst	1 FTE	
Office Assistant	1 FTE	
Technology Services Assistant	1 FTE	
Subtotal	8 FTE	\$500,851

These compensation figures do not include the cost of benefits

In addition to the positions noted above, the high schools have acquired technicians, independent of the technology services department, to deliver technology support to teachers and site administrators. Therefore, the personnel costs shown above do not represent the full cost borne by the district for technology support services. Several school sites also use outside contractors to install infrastructure, which leads to extra expense, divergent technologies and a significantly more difficult technology support environment.

## Operations

Critical information systems, including the student information system, business system and human resources system, are not consolidated or located close to one another to facilitate maintenance. For example, the pupil services department supports the student information system, which is separate and distinct from other administrative systems. Duplicate data entry is required for many human resources functions. The lack of centralized data collection and dissemination poses unnecessary obstacles for users seeking quick answers to simple data requests.

There are no formal policies and procedures to guide technology support services. Support technicians are not assigned to specific school sites; instead, they begin each day with site visitations based on assignments given at the end of the previous day. This creates a situation in which support staff members commonly visit more than one school site during each workday. The time spent traveling between school sites severely hampers technician productivity. Site administrators expressed frustration that technology staff members are not assigned to provide site support on any planned or predictable schedule. A staff allocation plan would ensure that all sites receive support in a more structured and predictable manner by assigning staff to specific sites on specific days and making administrators aware of when technology support staff will be on site.

Some technology support staff members do not routinely check in with site personnel before leaving a campus after a repair is completed. A formal policy and procedures for technology support would help resolve this issue. For example, procedures could include a requirement that support technicians check in at the office when first arriving at a site and return to the site office after finishing the work to provide a progress report and an indication of when they will return to address any unresolved items. Technicians should also e-mail users about the status of incomplete work.

In addition to computers and related equipment, the technology department is responsible for supporting pagers, radios, cell phones, personal digital assistants, printers, faxes and various software applications.

Support requests to the technology services department are received by the technology services assistant and maintained within a FileMaker database. Without exception, technicians within the department indicated that the database is cumbersome to use and not very effective. Commercial web-based help desk systems are available that are much more efficient and easy to learn; many allow users to initiate support requests and check on the status of a support request.

Technology staff members commented that they try to have monthly department meetings to discuss district and department technology issues. Meetings are not guided by printed agendas, and staff members are not invited to share agenda items in advance of the department meetings. Regular meetings with a printed agenda provided in advance and opportunity for staff members to add agenda items would improve communication regarding district technology initiatives.

Several staff members indicated that they have not received an employee performance evaluation in several years. Performance evaluations define the high level of performance required and specify areas where improvement is needed. Without documentation, progressive disciplinary actions such as counseling sessions, written notices of unsatisfactory performance, suspension without pay, demotion, or termination of employment may not be possible to correct unsatisfactory performance.

Installation of new computers currently results in the older computers being shifted to another location to displace even older equipment, which in turn is moved to another location to replace even older equipment, and so on. Technology support technicians indicated that moving computers is particularly labor intensive because of the amount of time required to move equipment and reconfigure workstations. Limiting computer displacement to one time and taking out of service and making surplus any computers that have been displaced more than once would more clearly establish an end of life timeline for replacement of old computers. Useful parts such as hard drives can also be removed from computers being taken out of service.

The practice of displacing computers more than once in an attempt to replace progressively older computers has also resulted in a proliferation of aging computer equipment throughout the district. Technology services staff members estimate that approximately half of the 4,000 computers in the district are obsolete and incapable of running the newer operating systems and applications that users need. Because of this situation, a detailed plan for replacing obsolete equipment will have to be developed before implementing districtwide online attendance. In addition, the large number of obsolete computers exacerbates the perception among site administrators that technology support technicians are always behind and do not provide service in a timely manner.

The district's student information system (SIS) has never been backed up using standard backup procedures. The SIS data totaling approximately 140 megabytes is sometimes manually copied to a computer that is located next to the SIS server using file transfer protocol (FTP). Technology support staff indicated that this copy procedure is not automated, must be initiated manually, and is performed at least weekly. A restore of the SIS data is conducted monthly but is not tested. This situation represents a significant risk. The district's SIS data is not adequately protected and the district's primary revenue stream, which is generated from average daily attendance data, would be jeopardized in the event of a catastrophic loss or corruption of SIS data. An automated daily backup of the SIS data to the adjacent server, an automated tape backup system and regular test restore procedures would help resolve this issue.

Every new computer received by the district must be imaged by technology services department staff members to prepare it for use. Technicians do not take advantage of the low cost preimaging services offered by most manufacturers, which can reduce the amount of work that needs to be performed prior to installing computers.



## Recommendations

*The district should:*

1. Consider creating a new department called Information and Technology Services (ITS) that combines all aspects of educational technology, information technology and network services within a single department.
2. Consider creating a new position of Chief Technology Officer (CTO) to assume control of all aspects of administrative and instructional technology. Ideally, the CTO should report directly to the superintendent, and consideration should be given to making the position a cabinet-level position. A sample CTO job description is included as Appendix A.
3. Establish a district technology committee (DTC) to guide planning, standards development and support activities. The DTC should include representatives from administrative, instructional and classified employee groups, and the community. The CTO should attend all DTC meetings and provide updates on the department's progress toward stated goals. The CTO should understand that the DTC has advisory authority to direct technology department activities and should ensure that the committee's standards, specifications, and recommendations are carried out. The primary focus of DTC meetings should be on increasing communication and collaboration in technology-related decisions and operations. The DTC should be charged with improving communications, developing hardware and software standards, reviewing all purchase orders for non-standard technology items, and managing technology department activities. For example, the DTC should examine the district's Internet filtering policies and should begin discussing replacement of the student information system. In addition, the DTC should develop a clear vision and strategies for using Web-based resources to achieve instructional objectives.

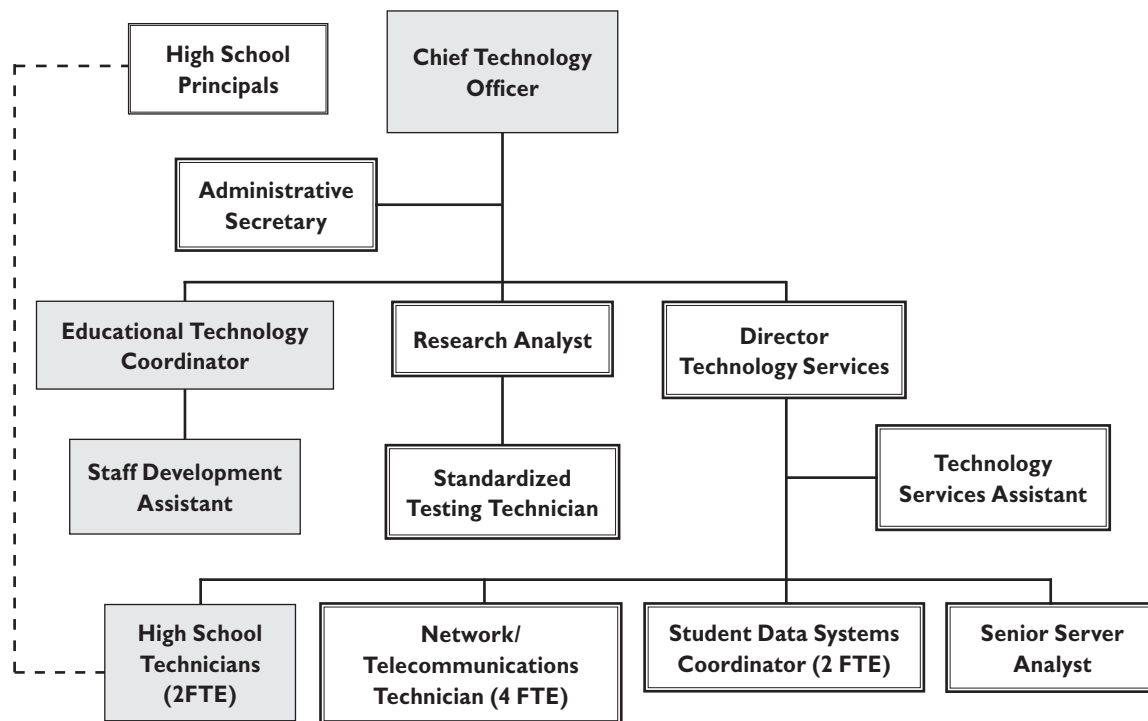
The DTC should also develop standards related to Web content and Web-based curricula. These standards should address the following:

- Define the district's objectives for its Web site.
- Define standards for keeping the Web site current.
- Identify employees who will be responsible for Web content and maintenance.
- Identify training requirements and who will be responsible for providing training.
- Develop a timeline that includes training, Web content development and milestones related to desired outcomes.
- Define Web content standards that focus on information and student success while allowing individuals and departments the access needed to profile sites and departments.

The DTC should rely on technology department recommendations to guide the process of developing specifications and standards. Meetings should be guided by a printed agenda that is prepared in advance and should be co-chaired by the CTO and an instructional staff member, with all members invited to submit agenda items prior to each meeting. Other technology department staff members should occasionally attend DTC meetings to gain an increased awareness of the primacy of education and how technology services fits into the district's mission and objectives. FCMAT believes that a collaborative relationship between technology support staff and the DTC will be of great benefit to the district, particularly during the planned conversion to a new student information system.

4. Consider the organizational chart presented below as the proposed ITS department structure.

*Information and Technology Services*



- Represents new positions
- Represents existing positions
- Represents eliminated positions (detailed below)

Some of the positions from the formerly independent departments are not depicted in the organizational structure shown above.

Any changes to positions should be carried out through the collective bargaining process with the appropriate bargaining unit.

Information regarding the positions recommended for elimination is as follows:

- Consider eliminating the position of Director of Student Assessment position. Duties previously performed by this position should be reassigned to the Student Data Systems Coordinator positions (estimated salary savings: \$106,922).
- Consider eliminating the position of Senior Office Assistant that reports to the Director of Student assessment Services position (estimated salary savings: \$50,000).
- Consider eliminating the position of Office Assistant that reports to the Technology Services Director position (estimated salary savings \$33,322).

The annual salary savings associated with the three eliminated positions would be \$190,244.

Information and various rationale regarding recommended changed and new positions is as follows:

- Consider transferring the administrative secretary from the student assessment services department to the new information and technology services department, reporting directly to the CTO.
- Consider creating a new position titled Educational Technology Coordinator (ETC). The primary focus of the ETC should be on instructional technology and professional development for certificated staff. This position will significantly improve the delivery of instructional technology services and staff development throughout the district.
- Consider creating a new position titled Staff Development Assistant, reporting to the ETC.
- Consider reassigning the research analyst position to report to the new CTO.
- Consider reclassifying and reassigning the student data systems coordinator position to a standardized testing technician, reporting to the research analyst.
- Consider reassigning the technology services director to report to the CTO.
- Consider creating two high school site-based technician positions.

Consider approximate salary placements for the Information and Technology Services department as follows:

<i>Position</i>	<i>Cost per FTE</i>	<i>Total</i>
Chief Technology Officer	\$108,000	\$108,000
Administrative Secretary	\$41,000	\$41,000
Educational Technology Coordinator	\$96,000	\$96,000
Staff Development Assistant	\$35,000	\$35,000
Director, Technology Services	\$96,000	\$96,000
Technology Services Assistant	\$42,000	42,000
Senior Server Analyst	\$75,000	\$75,000
Student Data Systems Coordinator (2)	\$49,000	\$98,000
Network/Telecommunications Tech (4)	\$61,000	\$244,000
High School Site-Based Technician (2)	\$61,000	\$122,000
Research Analyst	\$54,000	\$54,000
Standardized Testing Technician	\$42,000	\$42,000

Total Cost for above 17 FTE positions: \$1,053,000

Total cost for 15 FTE positions, without  
high school site-based technicians: \$931,000

Current Allocation for Tech and Assessment: \$838,581

5. Discontinue allowing school sites to hire technology support personnel or to contract independently with outside vendors for assistance with technology infrastructure projects.
6. Place all critical information systems, including the student information system, business system and human resources system, reasonably close together to make maintenance easier. Responsibility for all major systems should reside within the newly organized Information and Technology Services department.
7. Define and implement a formal policy and procedures for providing technology support.
8. Develop a staff allocation plan that ensures that all sites receive support in a structured and predictable manner and that makes administrators aware of when technology support staff will be on site. Site support assignments should be interrupted only in case of an emergency.
9. Consider replacing the existing FileMaker database help desk system with a user-friendly commercial, web-based help desk system that allows users to initiate and

- check support requests. Ensure that the CTO and end users are included in the evaluation and selection of the new system.
10. Ensure that the Information and Technology Services department conducts regular meetings to improve communication regarding technology initiatives. Agendas should be printed in advance and staff should be given the opportunity to add agenda items.
  11. Ensure that information technology services department staff members receive annual performance evaluations.
  12. Limit to one the number of times that displaced computers can be used to replace even older computers.
  13. Implement standard, automated daily backups of the student information system to the adjacent server and to tape, and conduct occasional test restores of the backups.
  14. Communicate with hardware vendors to arrange for preimaging of computers directly from the manufacturer.



## ***Policies***

The district lacks an equipment replacement strategy. Funding for equipment replacement is a major concern for site administrators, who acknowledge the need to update aging and obsolete computer equipment. Computers that are more than five years old are slow and cannot run the latest software or operating systems. A commonly accepted strategy is to replace a percentage of equipment each year. For example, replacing the oldest 20% of all district equipment annually would result in all the district's computers being replaced every five years. This would help provide better standardization of equipment; allow for more accurate technology budgeting and planning; and reduce both support costs and, as a result, the total cost of ownership.

The district lacks an equipment disposal policy for handling surplus computers, faxes, copy machines, cell phones and other electronic equipment. A disposal policy would provide guidelines to ensure that hard drives are wiped clean to ensure the privacy of sensitive district information. In addition, the district lacks a donation policy that would provide standards for computer equipment donated to the district.

Many district staff members have never signed an acceptable use policy (AUP) that defines district policy for acceptable and unacceptable use of district network resources such as Internet and e-mail. The respective school sites maintain acceptable use policies signed by students. Developing separate board-approved AUPs for staff and students and reviewing them every two years can help ensure that they remain up to date and minimize liability. Providing every employee and student with a complete copy of their respective AUP and requiring a signature every year in order to gain network privileges can also improve communication and reduce liability.

An effective practice is for managers and department heads to be responsible for ensuring that employees in their respective departments and areas return a signed AUP each year, and for students to be granted a network login only after receiving the entire AUP and signing it.

The district lacks documented password policies and other security protocols to safeguard access to administrative systems such as the student information system (SIS). In addition, users are not trained in security issues. Training users can help improve password and network security. For example, training in password memorization techniques helps reduce the risk of teachers and staff writing their passwords down and storing them at or near their computer workstations. In addition, setting passwords to expire and implementing password history checking can ensure that passwords are changed regularly and not reused.

**Recommendations**

*The district should:*

1. Develop an equipment replacement strategy that includes replacing the oldest 20% of all district computer equipment each year.
2. Develop a computer equipment disposal policy. A sample disposal policy is included in Appendix B.
3. Develop an equipment donation policy that defines minimum specifications for donated computer equipment. Hardware that does not meet minimum standards should be rejected. A sample donation policy is included in Appendix C.
4. Create separate board-approved AUPs for staff and students, and review the policies every two years.
5. Require every employee and student to sign an AUP before the start of each school year in order to receive network privileges.
6. Implement regular user training to raise awareness of security issues, including password security. Users should be trained in password memorization techniques.
7. Implement password history checking to ensure that passwords are not reused, and password aging to ensure that passwords expire at least every 120 days.



## *Planning and Standards*

For many years, district sites have planned and purchased technology assets independently. As a result, disparate, incompatible systems have been implemented and the advantages of collective purchasing power have been lost. Technology department staff members expressed frustration regarding the difficulty of establishing a firm standard for hardware acquisition. For example, technology services staff may recommend a certain product to site administrators, but the recommendation is often ignored simply because the site administrator pursues similar equipment that can be acquired at a lower cost. In these situations, technology services department recommendations have not been enforced, allowing sites to bypass the department's efforts to achieve hardware standardization.

The presence of nonstandard equipment on a network creates additional support costs: technicians have to carry twice the number of software drivers, create twice as many images for a computer that has malfunctioned, and receive twice the amount of training to support the additional nonstandard equipment. Increased coordination of technology purchases would reduce expenditures, benefit schools and departments, and save site resources.

Despite the perception that the district has a culture of decentralization and that most sites would strongly resist efforts to standardize hardware and software, site administrators agreed without exception that they would be willing to set aside their individual preferences to assist the district in its efforts to standardize equipment and improve service delivery. FCMAT believes that standardization is critical to improving the efficiency and effectiveness of technology services support.

The district's technology plan was recently updated by a limited number of staff, without input from a variety of district stakeholders. During interviews, users characterized the existing technology plan as "shelf dust" and expressed a perception that the plan does not accurately reflect the district's vision and goals with respect to technology. Because technology support staff members were not involved in creating the existing plan, it does not address the priorities of technology service. Technology support staff members indicated that they would like earlier involvement in instructional decisions related to technology. In addition, none of the district sites have created site technology plans that support districtwide technology goals and initiatives.

Although the development of the technology plan may have been expedient for grant and E-Rate funding requirements, the lack of broad participation in the creation of the plan significantly limits its credibility and usefulness as a guiding document for the district.

Best practices for technology planning suggest that a technology planning team be comprised of representatives from many groups, including students, parents, teachers, library media specialists, resource specialists, site administrators, district administrators (curriculum and technology), classified staff, community leaders, business representatives and partners from higher education.

The district lacks a broad-based technology committee that meets regularly and is chaired by a district instructional technology leader. It has no effective tool for reviewing and updating the technology plan and addressing other key technology issues including, but not limited to, the following:

- Internet filtering
- Web site content and maintenance
- Web-based application use standards
- Training and professional development

District and site administrators expressed concern regarding where to find funding for computer upgrades. The technology budget is not aligned with a long-term plan; it is funded with available district resources and staff indicated that it is frequently used for projects other than technology.

The lack of enforced standards has also increased support problems for user services staff members, who are often first made aware of a technology project only when installation problems occur and they are contacted for support.

Some school sites have not set aside funds for equipment replacement. A disparity in funding for individual school sites has resulted in some sites being replete with technology while others are left struggling to find funds for critical equipment replacement. The loss of Digital High School (DHS) funding was a significant setback for both of the district's comprehensive high schools.

Although the vast majority of the district's users have Novell GroupWise e-mail accounts, a few still use the district-hosted imail POP3 e-mail client and are unable to take advantage of the groupware features contained within GroupWise, including calendar sharing and shared resource scheduling.

### ***E-Rate***

The district's director of technology services maintains E-Rate applications and documentation. The process of applying for E-Rate discounts is complex; users must be thoroughly familiar with technology and the numerous strict application filing deadlines. Many school districts contract with E-Rate consultants to maximize their discounts and minimize the delays associated with inquiries from representatives of the organization that oversees this federal discount program. E-Rate consultants typically charge either a flat rate per year or a very small percentage of the discount the district receives, with a "not to exceed" provision established in advance. E-Rate consultants used by other school district and county offices of education include, but are not limited to, the following:

Kim Friends  
 California School Management Group  
 3333 Concourses, Suite 4102  
 Ontario, CA 91764  
 (909) 944-7798  
 kfriends@csmgconsulting.com  
 www.csmgconsulting.com

Fred Brakeman  
 Infinity Communications & Consulting, Inc.  
 1800 30th Street, Suite 175  
 Bakersfield, CA 93301  
 (661) 716-1840  
 fbrakeman@inifinitycomm.com  
 www.inifinitycomm.com

## Recommendations

*The district should:*

1. Ensure that technology standards are enforced throughout the district. All technology requisitions should be forwarded to the CTO for approval. This will help improve standardization and keep support requirements to a minimum. Technologies that are not compatible with existing standards should be considered on a case-by-case basis. Nonstandard requests that are deemed justified should be granted; however, the CTO should first meet with the user to determine if existing standards can be maintained.
2. Charge the district technology committee (DTC) with the development of a new strategic technology plan. Participation should include classified, certificated and management personnel, parents, community members and student representatives. A list of committee responsibilities should be developed, including the following:
  - Reviewing site technology plans.
  - Reviewing the goals and objectives of the information and technology services (ITS) department.
  - Exploring available funding sources.
  - Exploring available educational systems.
  - Submitting a proposed technology plan and budget to the governing board for consideration.
3. Associate the ITS department budget with objectives outlined in the new strategic plan.
4. Ensure that ITS department staff members are involved in all stages of technology evaluation, selection, and implementation.
5. Ensure that all school sites set aside appropriate funds for equipment replacement. Disparities in technology infrastructure between school sites should be eliminated by allocating the funds needed to bring all school sites to the same level with respect to technology infrastructure and technological capabilities.

6. Ensure that all users in the district have access to GroupWise e-mail accounts; eliminate the use of the imail POP3 e-mail application.
7. Consider contracting with an experienced E-Rate consultant to assist with completing applications and ensuring that critical time lines and submission deadlines are met.

## *Instructional Technology*

During interviews, technology services staff members acknowledged that their efforts do not integrate with the objectives and initiatives of instructional users. Eighty percent of teachers indicated that they never work with colleagues to implement technology and infuse technology into the curriculum. Teachers operate independently of each other. For example, there are no gradebook standards, so grade reporting is not consistent.

Instructional applications are adopted without sufficient input or participation on the part of technology services support staff members. For example, even though there was significant advanced planning for implementation of the READ 180 reading intervention software, support staff members only recently learned that the district had purchased the software and that instructional staff wanted it installed by the beginning of summer school. The lack of awareness is an indicator of insufficient collaboration and communication between instructional staff and technology services staff members. A more collaborative approach for the adoption of software would improve decision making, help ensure compatibility among existing systems and help the technology services department determine and meet ongoing support requirements.

Several instructional staff members commented that the district needs to update the computer equipment in classrooms. This finding relates to the previously mentioned need to develop an equipment replacement strategy that addresses both administrative and instructional equipment.

In 2002, the district's full time teacher specialist position for professional development was eliminated and the training center previously located at the Rincon school site was repurposed. Another instructional staff member has assumed some of the instructional technology support functions and has been involved with the adoption of instructional technologies, including working with publishers to implement staff development to support the new technology-infused curriculum now available for adoption. However, the response among instructional staff has not been good. Only eight or 10 of the district's more than 500 instructional staff members took advantage of the training opportunities.

Many instructional staff members commented that it is difficult to adopt instructional technology standards in an environment where there is little enforcement. Technology standards need to be enforced if the district is to develop the content standards that will lead to improvements requested by the district's board members.

The district's student assessment management software, EduSoft, is underused. The district office has not assigned a staff member to provide support for the EduSoft system, and instructional staff members have not received sufficient training to enable them to take advantage of EduSoft to improve student achievement. In fact, the district has no staff member assigned to provide overall vision or coordination of educational technology activities. Some staff members commented that a position of this type has existed in the past but was eliminated because of budget constraints. In addition, the facility previously made available for staff and professional development activities was repurposed.

With the exception of a few in-service sessions provided by vendors, there is no staff development plan related to educational technology and no opportunities to improve instructional use of technology.

### ***Recommendations***

*The district should:*

1. Develop a more collaborative approach to the adoption of instructional software. Technology services staff members should be included early in the process of evaluating and selecting instructional software applications.
2. Charge the educational technology coordinator (ETC) with responsibility for the integration of technology into instruction. The ETC should develop a long-term strategic plan to accomplish this goal. The ETC should be included in all discussions that involve the acquisition and support of educational software and hardware. In addition the ETC should be responsible for providing support for all educational systems, including the READ 180 and EduSoft applications.
3. Ensure that the ETC develops a comprehensive staff development program that is based on current needs and that contains clear objectives for improving the use of instructional technology. Particular attention should be given to training related to major software acquisitions such as EduSoft and READ 180.
4. Assign the staff development assistant the responsibility of developing training on the EduSoft system for instructional staff members. The staff development assistant should work with the ETC to develop an overall vision for the use of EduSoft that will allow the district to improve student learning and achievement.
5. Place a high priority on updating obsolete equipment in classrooms first.
6. Charge the staff development assistant, reporting to the ETC, with responsibility for reinvigorating professional development efforts aimed at instructional staff members.
7. Ensure that the ETC has appropriate authority to enforce instructional technology standards.

## *Administrative Technology*

As mentioned previously, standard backups of the district's student information system (SIS) server have never been performed, which presents a significant vulnerability that merits immediate corrective action.

The district lacks detailed implementation plans for most of its major technology initiatives, including further distribution of the Aeries Browser Interface (ABI), online attendance, Gradebook and grade reporting applications. At present, sites are allowed to decide whether or not to implement the SIS-based Gradebook and grade reporting applications. Further complicating this issue, the district has purchased and implemented an application called ReportCard Maker, the selection of which indicates a lack of awareness regarding the capabilities of the current SIS and a lack of coordination with technology support staff. The exception to this finding is the district's rollout of the READ 180 application, which is likely to go smoothly because of significant application rollout planning.

During interviews, administrators indicated that there are problems with the state reporting of student information. These problems can be traced back to software used by personnel staff members that is, by one administrator's estimate, several generations old and can no longer be updated. It is likely that the county office-hosted financial system, which includes a personnel module, could perform the functions currently performed by the personnel software.

Site administrators expressed frustration that they do not have online access to purchase order and budget information. Instead, they must rely on monthly paper-based budget reports. The lack of timely and accurate data has forced administrators to devise alternative systems using QuickBooks and Excel to better track budget information.

## *Recommendations*

*The district should:*

1. As mentioned earlier, ensure that the SIS data is backed up daily using standard, automated backup procedures.
2. Develop detailed implementation plans for all major technology initiatives, including further distribution of the Aeries Browser Interface (ABI), online attendance, and Gradebook and ReportCard Maker grade reporting applications.
3. Consider eliminating the obsolete personnel software currently used by personnel staff members.
4. Provide site administrators with online access to purchase order and budget information. Once online access is made available, site use of alternative systems such as QuickBooks and Excel should be discontinued.





## *Network and Security*

FCMAT reviewed network elements at each district school site, including routers, switches and a complete scan of the district's globally routable IP address space. Although several wireless access points were observed, access to them was not provided; therefore, FCMAT's recommendations regarding wireless networks will be of a general nature.

The district lacks complete and accurate network documentation, and much of the hardware currently in use has been discontinued by the respective equipment vendors. In addition, most network hardware is not running the latest vendor-provided firmware.

Adequate network documentation typically includes a diagram of the overall network backbone, a diagram of the network at each network site, and a spreadsheet or other document that contains the following information for any telecommunication circuits used in the network:

- The "A" and "Z" location for each circuit.
- The "A" and "Z" location contact person name, e-mail address, and telephone number.
- The telecommunication provider circuit ID for each circuit.
- The trouble reporting contact telephone number for each telecommunication provider.

Complete network documentation also typically includes each network element's host name, IP address, vendor, vendor part number, serial number, firmware version, physical location, and the name, address and telephone number of a contact person at that physical location.

Best practices include monitoring whether or not current hardware is still supported, replacing hardware that is no longer supported by vendors, and updating firmware to help ensure that elements receive important performance and security-related bug fixes and enhancements.

There does not appear to be any separation of student/academic network traffic from administrative network traffic. This situation presents a potential data security risk. Network traffic containing private data, such as student information system data, should never be transmitted across an IP subnet that is also used to provide network access to students or other users not authorized to view private data. The district's current network configuration makes it possible for private data to be obtained by a network user who is not authorized to view this private data. There are several ways to create separate networks for each type of data, including a firewall configuration on each site router, or separate physical Ethernet interfaces combined with IP access lists.

Many network elements use the equipment vendor's default authentication settings for access to their management interface; network access to the management interface of these elements is not protected by an IP address access list. Vendor default usernames and

passwords are widely available on the Internet and can be used by an unauthorized user to gain access to an element's management interface.

Under the current configuration, it is possible for any computer on the district's network to connect to the management interface of every network element. Thus any computer user who accesses the element and has the passwords can potentially obtain complete control of the network element. All network-based access to the management interface of every network element needs to be restricted by an IP address-based access list that permits only a small number of management workstations to access the element. Network-based access includes Telnet, SSH and HTTP.

Many of the district's network elements are configured to provide access to their Simple Network Management Protocol (SNMP) interface with the default SNMP community strings of "public" and "private" rather than protecting SNMP access by means of an IP address list. These community strings are widely documented, easily available on the Internet, and could allow an unauthorized user to gain additional information about a network element or modify its configuration. Thus it is currently possible for any workstation in the network to obtain information from any network element that has SNMP enabled if the user knows the SNMP community string. In some cases it is also possible for the user to modify the configuration of the network element, or even reboot the network element, via the SNMP interface.

Common and comprehensive network security procedures include restricting access to SNMP community strings by use of an IP address-based access list that permits only a small number of management workstations to manage the network elements via SNMP. This arrangement ensures that only the IP addresses in the access list will be able to manage the network element via its SNMP interface.

Many of the district's network elements are configured to allow access to their management interface via the local auxiliary report without requiring a username or password. As a result, unauthorized users who have physical access to certain network elements can gain access to the management interface of those elements without providing a valid username and password. Requiring usernames and passwords is a standard network security procedure and needs to be implemented.

Remote network event logging is not enabled on any of the district's network elements. Best practices for network management include configuring all network elements to send event logs using the syslog protocol to a syslog server located on the network. The syslog server can be configured to automatically review the event logs and alert network administrators to potential or ongoing network problems. Another advantage of maintaining logs is that it helps create an audit trail that may be useful in the prosecution of a criminal case involving unauthorized access to the district's network. A mid-grade server running the Linux operating system or one of the freely available BSD UNIX operating systems usually makes a good syslog server.

Some of the district's network elements are configured to time-stamp event logs with the amount of time they have been running (uptime); no network elements have network time protocol (NTP) enabled. Because uptime varies from one element to another with no common reference, the use of network element uptime for log time-stamping results in logs that are of little value for troubleshooting network or element issues and of no use in the legal prosecution of unauthorized network access. A network time protocol (NTP) server can provide reliable time data for all network elements for both troubleshooting and legal needs. Accurate log time stamping can be of great importance in the legal prosecution of unauthorized network access. The NTP service can be provided by a mid-grade server running the Linux operating system or one of the free BSD UNIX operating system variants.

Authentication, authorization and accounting (AAA) are not enabled on any of the district's network elements. Enabling AAA on all elements that have this feature would allow the elements to use a central repository for username and password authentication. This arrangement places all network element access accounts on the AAA server rather than on each individual network element. An AAA system can also provide targeted access to support staff by enabling specific users to have access to specific commands. The use of AAA is also critical for creating an audit trail for the configuration of each network element. Many AAA configurations allow the recording of every individual command entered by each user, which can be very helpful for troubleshooting configuration-related network issues and for providing evidence to law enforcement personnel for the investigation and prosecution of unauthorized network access. The AAA service can be provided by a mid-grade server running the Linux operating system or one of the freely available BSD UNIX operating system variants.

None of the district's network elements are configured to display adequate login banners. Properly configured banners display legal language defining the privacy and monitoring expectations of any management interface access session. A properly worded login banner can be important in the legal prosecution of unauthorized network access or use. A sample login banner is included in Appendix D.

Many of the district's router interfaces are labeled as belonging to a "voice VLAN," but no IP quality of service policy is applied to these interfaces. Quality of service requirements vary from vendor to vendor, so the documentation provided with a voice over IP (VOIP) system can be used to determine which traffic needs to be prioritized on the network. Voice over IP traffic traveling through a router or Ethernet switch interface that is not configured for priority will result in degraded voice quality.

Many of the district's router interfaces are configured for automatic speed and duplex detection. It is common for a network element that is configured for automatic detection to improperly detect the port speed, the duplex, or both, resulting in a high error rate on that port and a severe degradation of network performance. Manual configuration of an Ethernet interface's speed and duplex settings to match those of the Ethernet switch port to which it is connected can resolve this issue.

Most of the district's network uses globally routable IP address space. The use of globally routable IP address space in a private enterprise network has been discouraged since the release of request for comments (RFC) 1918, which allocated specific blocks of IP address space for use by private enterprise networks. Using RFC 1918 address space makes firewall configuration easier and ensures that a mistake in configuring the network firewall will not result in the entire network being exposed to the global Internet. Migrating the district's network to RFC 1918 address space is needed for increased security but is a time consuming process for network management staff.

A remote scan of the district's globally routable IP address space found seven hypertext transfer protocol (HTTP) servers that currently permit connections from the global Internet. This is likely by design, as these HTTP servers probably provide information that is available to the general public. The scan also detected one file transfer protocol (FTP) server, one simple mail transfer protocol (SMTP) server, and one Apple filing protocol (AFP) server. The AFP server is displaying its name as "Bob Houghton's Power Mac G4; protocol 3.2; Max OS X 10.4.\*." This name may not be desirable and should be reviewed. Reviewing firewall policies at least quarterly can help ensure accuracy and adherence to the district's security policies.

As mentioned earlier, access to the district's wireless access points was not provided. As a result, FCMAT was not able to determine the wireless protocols in use. Good wireless security practices include discontinuing any existing use of wired equivalent privacy (WEP) encryption and using wireless access points that support the 802.11i standard, which enables the highest level of security currently available in a 802.11 wireless network. WEP can be easily defeated with free software available from many Internet sites. A paper located at <http://eprint.iacr.org/2007/120.pdf> details how the authors were able to successfully break WEP keys in less than 60 seconds and thereby gain full access to a wireless network.

**Recommendations:**

*The district should:*

1. Create complete and accurate network documentation as soon as possible, and review the documentation for completeness and accuracy at least quarterly.
2. Replace all currently operating network hardware that has been discontinued by the network element manufacturer, and replace currently installed Ethernet hubs with Ethernet switches.
3. Review the vendor support status of each network element at least quarterly.
4. Ensure that all network elements are running the latest vendor-provided and vendor-certified firmware release, and review the status of available firmware updates at least quarterly.
5. Establish separate networks for student data and district administrative data such as student information system data. The use of secondary IP addressed Ethernet interfaces should be discontinued.
6. Remove or change the vendors' default usernames and passwords on all network elements.
7. Change the default SNMP strings on network elements that are currently using the "public" and "private" string defaults.
8. Implement an IP address-based access list to limit network-based access to the management interface of every network element. Access should be restricted to a small number of management workstations.
9. Implement an IP address-based access list to limit network-based access to SNMP community strings. Access should be restricted to a small number of management workstations.
10. Ensure that local access to the management interface of all network elements is configured to require a username and password, and ensure that passwords are changed frequently.
11. Install and configure a syslog server on the network and configure all network elements to send event logs via the syslog protocol to the syslog server. The syslog server should be configured to automatically review the event logs and alert network administrators to potential or ongoing network problems.
12. Configure all network elements to synchronize their clocks with a network time protocol (NTP) server and to time-stamp their event logs with the time provided to them by the NTP server.
13. Configure AAA on every network element that supports it, and configure an AAA server.

14. Configure any router or Ethernet switch interface that carries voice over IP (VOIP) traffic to apply IP-based quality of service to this voice traffic. The documentation that came with the VOIP system should be consulted to determine which network traffic needs priority.
15. Manually configure the speed and duplex settings of any router Ethernet interface to match those of the Ethernet switch port to which it is connected.
16. Migrate the district's network to RFC 1918 address space to eliminate the use of globally routable IP address space. Allocate the staff time needed for this task.
17. Develop a login banner with adequate legal language defining privacy and monitoring expectations, and ensure that each network element that supports a login banner is configured to display one for all network management interfaces that the network element supports.
18. Consider reviewing and changing the name of the AFP server.
19. Review all firewall policies at least quarterly to verify accuracy and ensure adherence to the district's security policies.
20. Ensure that all wireless access points fully support the 803.11i standard, and eliminate the use of WEP encryption, if any.

# Appendices

## *Appendix A*

### *Sample Chief Technology Officer Job Description*

## APPENDICES



## Appendix A

### Sample School District Sample Job Description

JOB TITLE: Chief Technology Officer, Information and Technology Services

#### SUMMARY

Under the general direction of the Superintendent, assumes primary management responsibility for the Information and Technology Services Department; ensures efficient delivery of information system services and technology resources for users districtwide; and performs other essential job-related work as required. The fundamental objective of this position is to ensure that computers and technology efforts are consistent with the overriding objective of effective delivery of quality educational services for the students, parents, and community.

#### DUTIES AND RESPONSIBILITIES

The following are examples of duties related to this position:

1. Plans, organizes, leads, directs, develops, and monitors all aspects of the Information and Technology Services Department; supervises Educational Technology Coordinator and other departments and provides direction to coordinators and supervisors of the Technology Services Department.
2. Directs and facilitates ongoing districtwide needs assessment and development of technology implementation plan to ensure delivery of efficient and effective day-to-day and ongoing information system and technology services districtwide.
3. Directs research, evaluation, assessment and testing functions, and district standardized testing program.
4. Oversees, develops, and implements the district plan for information systems and technology. Sets policy for the purchase and repair of computers, peripherals, and audiovisual equipment.
5. Directs, facilitates, and monitors information system implementation efforts to ensure that the Department keeps pace with day-to-day and future needs. Assures compliance with graduation requirements. Guides and assists departments and sites in the development of appropriate educational technology implementation and curriculum.
6. Maintains frequent group and one-on-one communication and works in a collaborative manner with department directors and other administrators and professionals districtwide to facilitate decision making and problem solving in the area of computers and technology services and assessment.
7. Oversees progress toward objectives relating to migration and other project management efforts.
8. Oversees the management of the interconnection of operating systems, desktop computer applications, network protocols, and mainframe applications.
9. Reviews, monitors, and facilitates negotiations with vendors and agencies to provide cost-effective resources in terms of day-to-day demands and longer term goals and

objectives.

10. Complies with applicable state, local, and federal rules, regulations, and laws, as well as the policies and procedures of the district.
11. Establishes and maintains effective working relationships with a variety of groups, including teachers, students, administrators, coworkers, vendors, consultants, and others as required.
12. Demonstrates and models safe, prudent, and healthful work behaviors and practices; identifies and works toward the elimination of unsafe or unhealthful work area conditions.
13. Performs other essential job-related work as required.

## SUPERVISORY RESPONSIBILITIES

Assign and supervise of all Information and Technology Services Department employees. Carries out supervisory responsibilities in accordance with the districts policies and applicable laws. Specific requirements include, but are not limited to, the following:

1. Manages substantial data bases and other information such that the quality, quantity, time lines, and facility of data retrieval and reporting support district and site needs.
2. Manages resources so that Information Technology Services Department provides timely and essential customer service, training and user support.
3. Utilizes knowledge sufficient to manage complex data base systems, network management [LAN and WAN environment] and protocols, intranet and Internet access, mini-computer operations, and multiple hardware and software platforms.
4. Manages and directs systems that support and assist users at all sites in computer, software, network, and system functions.
5. Develops and manages long-range planning for technology, infrastructure, and network environment to facilitate technology use districtwide.
6. Manages services that provide support through multiple methodologies, including but not limited to, help desk, on site training, equipment repair, and essential data retrieval for management purposes.
7. Clearly commands knowledge and expertise sufficient to facilitate the data needed to support the district's fiscal services, business services, human resources, and student services departments and/or divisions.
8. Manage districtwide network that supports voice, video and data transmission.

## QUALIFICATIONS

### Education and Experience

Administrative Credential - master's degree preferred.

Evidence of successful experience and management expertise in an educational setting or similar-sized organization involving computers and technology management.

## KNOWLEDGE, SKILLS, AND ABILITIES

Typical qualifying knowledge, skills, and abilities would include:

Knowledge, skills, and abilities in the area of information systems and technology resources; principles, practices, and languages used in communication oriented computer systems and programming; the capabilities, capacities, and limitations of computers and peripheral equipment; comparative equipment, planning, and cost control; principles and practices of accounting, statistics, and school district organization, activities, and requirements; principles of administration, human resource administration, departmental budgeting, supervision, and training.

**Language Skills.** Ability to read, analyze, and interpret common scientific and technical journals, financial reports, and legal documents. Ability to respond to common inquiries or complaints from customers, regulatory agencies, or members of the business community. Ability to write speeches and articles for publication. Ability to effectively present information to top management, public groups, and/or Governing Board.

**Mathematical Skills.** Ability to apply advanced mathematical concepts to resolve managerial issues and problems. Ability to understand mathematical operations for such tasks as schedules, time lines, hourly commitments, payrolls, probable outcomes, and forecasting *I* estimating.

**Reasoning Ability.** Ability to define problems, collect data, establish facts, and draw valid conclusions. Ability to interpret an extensive variety of technical instructions in mathematical or diagram form and deal with several abstract and concrete variables.

**Physical Demands.** The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

While performing the duties of this job, the employee is frequently required to walk and sit. Equal time needs to be spent observing employees job performance and accomplishments versus being assigned to only office work on an eight hour basis.

## WORK ENVIRONMENT

Work is performed primarily inside an office or office/laboratory environment with occasional exposure to the elements and cleaning solvents/chemicals. Requires occasional lifting of up to 50 pounds and the full range of fingering, talking, hearing, visual, and other physical and mental work demands.



*Appendix B*  
*Sample Equipment Disposal Policy*

## APPENDICES

## **Sample Computer Equipment Disposal Policy**

All surplus district-owned computers, faxes, copy machines, cell phones, and other electronic equipment with printed circuit boards shall be recycled by the district's selected and approved vendor. In addition, all computers or servers declared surplus that contain hard drives shall be wiped clean to at least DOD Level 3 or shall be destroyed by magnetic degaussing.

### **Rationale:**

The State of California recently determined that discarded televisions and computer monitors are classified as hazardous waste, unless properly recycled by a state licensed facility. Monitors and terminals contain from 4 to 8 pounds of lead, and circuit boards of both computers and printers contain lead solder, mercury and cadmium. The proper disposal of this equipment is essential to avoid liability and to be an environmentally responsible corporate citizen. In addition, computer hard disks may contain personal, confidential, and legally protected information that is still readable even when the files have been erased or the hard drive reformatted. Failure to destroy this information could lead to unauthorized access, identity theft, and liability to the district.

The key points of this policy include:

1. All non-working /obsolete computer products should be disposed of in an environmentally sound manner
2. Monitors and terminals are always a hazardous waste (or household hazardous waste, if from household use).
3. Other components of a computer system (e.g., circuit boards, keyboards, mice) could be hazardous depending on their lead, mercury, or cadmium content, which can vary from product to product.

### **Procedure:**

- Sites or departments that wish to declare computer equipment surplus shall send an email to the Technology Department listing description, serial number, asset tag number, and operational condition of the unit(s).
- Equipment will be picked up by Technology Department staff.
- Technology Department staff will package and ship the equipment to a center where it will be recycled in an environmentally safe and responsible manner.
- The hard drive will be overwritten to at least DOD Level 3 standards, or will be destroyed by magnetic degaussing upon request.





*Appendix C*  
*Sample Equipment Donation Policy*

## APPENDICES

## **Sample Computer Equipment Donation Policy**

Rowland Unified School District (RUSD) appreciates offers to donate used computer equipment. The following guidelines apply to acceptance of donated equipment.

1. All equipment accepted by RUSD should be in good working order. If the equipment is not in good working order, the accepting department or school assumes responsibility for the costs of putting the equipment in good working order.

Comment: Often a donor wishes to dispose of equipment that is not in working order. They may have the belief that giving it to RUSD is a positive way to dispose of it and that the district can make use of it. Unfortunately, there are often significant costs the district would incur to return the equipment to working order. For this reason, it is generally advisable to decline equipment that is not in initial good working order. Technology department staff members may be able to assist district personnel in determining whether a potential donation is in good working order.

2. Whenever possible, accept only equipment that is supported by RUSD, as defined in the hardware and networking sections of the district Technology Plan document. If the equipment is fully supported by RUSD and is in good working order when received, then the district will maintain the equipment just as if it had been originally purchased by the district. If the equipment is not a supported item, the school or department that accepts the donation assumes responsibility for costs of keeping the equipment in good working order.

Comment: Costs for repairing a piece of equipment that the district does not service can be substantial. Replacement of a computer motherboard or hard disk drive, for example, could cost more than the actual value of the equipment itself. In some cases, donated equipment can be viewed as “disposable,” with the intent to use it until it ceases to function, and then dispose of it.

3. Technology department staff members can assist with the setup and configuration of donated equipment that complies with the district hardware standards. For equipment that does not comply with the standards, technology support technicians can assist with the setup and configuration as long as the time required does not substantially exceed what would be required to set up equipment that is in compliance with district standards. If the technicians determine that extraordinary time will be required to set up and configure a non-standard piece of hardware, they will advise the accepting department or school that assistance will not be available.

Comment: Non-standard equipment can present serious challenges when interconnecting with district systems and networks. A substantial amount of time can be spent trying to locate software drivers and troubleshoot systems to make

them work properly with other district systems. At some point the time invested to set up and configure the equipment exceeds the value of the equipment.

3. Donated network equipment should not be connected to the district network without specific permission and direction from district network support technicians. Donated computers should only be connected to a network after review and approval by district technicians.

Comment: Networks are complex systems that require careful design and maintenance. The district strives to install networks that will be reliable and stable. A piece of networking equipment that is malfunctioning or improperly installed can destroy the integrity of the entire network and cause a network failure that impacts many students, staff and services. Under no conditions should anyone connect a hub, switch, router, or other device that affects the topography of a network without direct permission and direction from district network support technicians. Donated computers may contain network cards that are incompatible with district systems. Always check with an IT technician before attempting to connect an untested device to the network. Failure to do this may cause failure of your site network or even the entire wide area network. Technology department technicians are instructed to remove and/or confiscate unauthorized devices connected to any district network.

4. Make sure the donor provides software licenses for any donated software, including the operating system software.

Comment: The district makes every effort to be in compliance with copyright laws. If software is loaded on a computer, proof of ownership or license for that software must also be provided. It is not uncommon for a donor to donate a computer that has the Windows operating system and copies of other commercial software already installed. Without proof of license, these software items must be removed or purchased by the district. Since every computer requires an operating system, be sure to understand if you are getting a license for Windows with the computer (Macintosh computers always retain their original OS license), or if the donor has retained the license. If the donor has retained the license for Windows (or never had a legal license), a copy will need to be purchased before the computer can be used. This cost should be considered before accepting the donation.

5. If the donor requires a receipt for their donation, provide them with a letter listing the make, model and serial number of donated items. It is the responsibility of the donor, not RUSD, to determine the value of donated items.

Comment: A simple thank-you letter that lists the items that have been donated are appreciated by most donors and useful in many cases for tax purposes. It is not the responsibility of RUSD personnel to provide the donor with the appraised value of the equipment.

7. Items offered for donation at the district level will be reviewed by technology department staff for acceptance. Distribution of donated items to departments or schools will be handled by Assistant Superintendent. A donor may choose to designate a specific school or department to receive the donated items. If undesignated, the Assistant Superintendent will determine appropriate distribution by an assessment of need, or by soliciting proposals for usage of the equipment and selecting the recipient(s) on the merit of their proposal(s). A school or department may accept a donation directly if guidelines in this document are followed.
8. Any donated computer equipment, regardless of value, or other items valued at over \$500 should be added to the fixed assets system. Final recipient of donated equipment should provide a list, including the source of the donation, serial numbers, descriptions, models, brands, and approximate values to appropriate personnel in the Business Office whereupon bar codes will be provided for the recipient to attach to the equipment for inventory control purposes.
9. Technology department staff members can answer questions about the advisability of accepting donations.



## *Appendix D*

### *Sample Login Banner*

## APPENDICES



## Sample Login Banner

\*\*\*\*\*

### NOTICE TO USERS

This is a (Your org here) computer system and is the property of (Your org here). It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, (Your org here), and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or (Your org here) personnel.

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

\*\*\*\*\*



*Appendix E*  
*Study Agreement*

## APPENDICES

**FISCAL CRISIS & MANAGEMENT ASSISTANCE TEAM  
STUDY AGREEMENT  
April 30, 2007**

The FISCAL CRISIS AND MANAGEMENT ASSISTANCE TEAM (FCMAT), hereinafter referred to as the Team, and the Rowland Unified School District, hereinafter referred to as the District, mutually agree as follows:

1. **BASIS OF AGREEMENT**

The Team provides a variety of services to school districts and county offices of education upon request. The District has requested that the Team provide for the assignment of professionals to study specific aspects of the Rowland Unified School District operations. These professionals may include staff of the Team, County Offices of Education, the California State Department of Education, school districts, or private contractors. All work shall be performed in accordance with the terms and conditions of this Agreement.

2. **SCOPE OF THE WORK**

A. **Scope and Objectives of the Study**

The scope and objectives of this study are to:

- 1) Assess the organization and operations of the district's technology services department and make recommendations for improvement.
- 2) Conduct a review of the district's instructional implementation of technology and make recommendations for improvement.
- 3) Conduct a review of the district's administrative technology implementation and make recommendations for improvement.
- 4) Conduct a computer network security review and recommend improvements to harden network security precautions and improve network performance.

B. **Services and Products to be Provided**

- 1) Orientation Meeting - The Team will conduct an orientation session at the District to brief District management and supervisory personnel on the procedures of the Team and on the purpose and schedule of the study.
- 2) On-site Review - The Team will conduct an on-site review at the District office and at school sites if necessary.
- 3) Progress Reports - The Team will hold an exit meeting at the conclusion of the on-site review to inform the District of significant findings and recommendations to that point.
- 4) Exit Letter - The Team will issue an exit letter approximately 10 days

after the exit meeting detailing significant findings and recommendations to date and memorializing the topics discussed in the exit meeting.

- 5) Draft Reports - Sufficient copies of a preliminary draft report will be delivered to the District administration for review and comment.
- 6) Final Report - Sufficient copies of the final study report will be delivered to the District following completion of the review.

3. PROJECT PERSONNEL

The study team will be supervised by Anthony L. Bridges, Deputy Executive Officer, Fiscal Crisis and Management Assistance Team, Kern County Superintendent of Schools Office. The study team may also include:

- A. Andrew Prestage, FCMAT Management Analyst
- B. Bradley L. White, FCMAT Technology Consultant
- C. Warren Williams, FCMAT Technology Consultant

Other equally qualified consultants will be substituted in the event one of the above noted individuals is unable to participate in the study.

4. PROJECT COSTS

The cost for studies requested pursuant to E.C. 42127.8(d)(1) shall be:

- A. \$500.00 per day for each Team Member while on site, conducting fieldwork at other locations, preparing and presenting reports, or participating in meetings.
- B. All out-of-pocket expenses, including travel, meals, lodging, etc. Based on the elements noted in section 2 A, the total cost of the study is estimated at \$8,500. The District will be invoiced at actual costs, with 50% of the estimated cost due following the completion of the on-site review and the remaining amount due upon acceptance of the final report by the District
- C. Any change to the scope will affect the estimate of total cost.

Payments for FCMAT services are payable to Kern County Superintendent of Schools-Administrative Agent.

5. RESPONSIBILITIES OF THE DISTRICT

- A. The District will provide office and conference room space while on-site reviews are in progress.
- B. The District will provide the following (if requested):
  - 1) A map of the local area
  - 2) Existing policies, regulations and prior reports addressing the study

- request
- 3) Current organizational charts
  - 4) Current and four (4) prior year's audit reports
  - 5) Any documents requested on a supplemental listing

- C. The District Administration will review a preliminary draft copy of the study. Any comments regarding the accuracy of the data presented in the report or the practicability of the recommendations will be reviewed with the Team prior to completion of the final report.

Pursuant to EC 45125.1(c), representatives of FCMAT will have limited contact with District pupils. The District shall take appropriate steps to comply with EC 45125.1(c).

6. PROJECT SCHEDULE

The following schedule outlines the planned completion dates for key study milestones:

Orientation:	May 22, 2007
Staff Interviews:	May 22, 2007
Exit Interviews:	May 22, 2007
Preliminary Report Submitted:	July 6, 2007
Final Report Submitted:	To be Determined
Board Presentation:	To be Determined

7. CONTACT PERSON

Please print name of contact person: Dr. Bob Wertz, Assistant  
Superintendent of Administrative Services

Telephone 626 854-8308 FAX 626 935-8460

Internet Address bwertz@mail.rowland.k12.ca.us

Dr. Maria G. Ott 5/8/07  
Dr. Maria G. Ott, Superintendent Date  
Rowland Unified School District

Barbara Dean, Deputy Administrative Officer Date  
Fiscal Crisis and Management Assistance Team

In keeping with the provisions of AB1200, the County Superintendent will be notified of this agreement between the District and FCMAT and will receive a copy of the final report.