

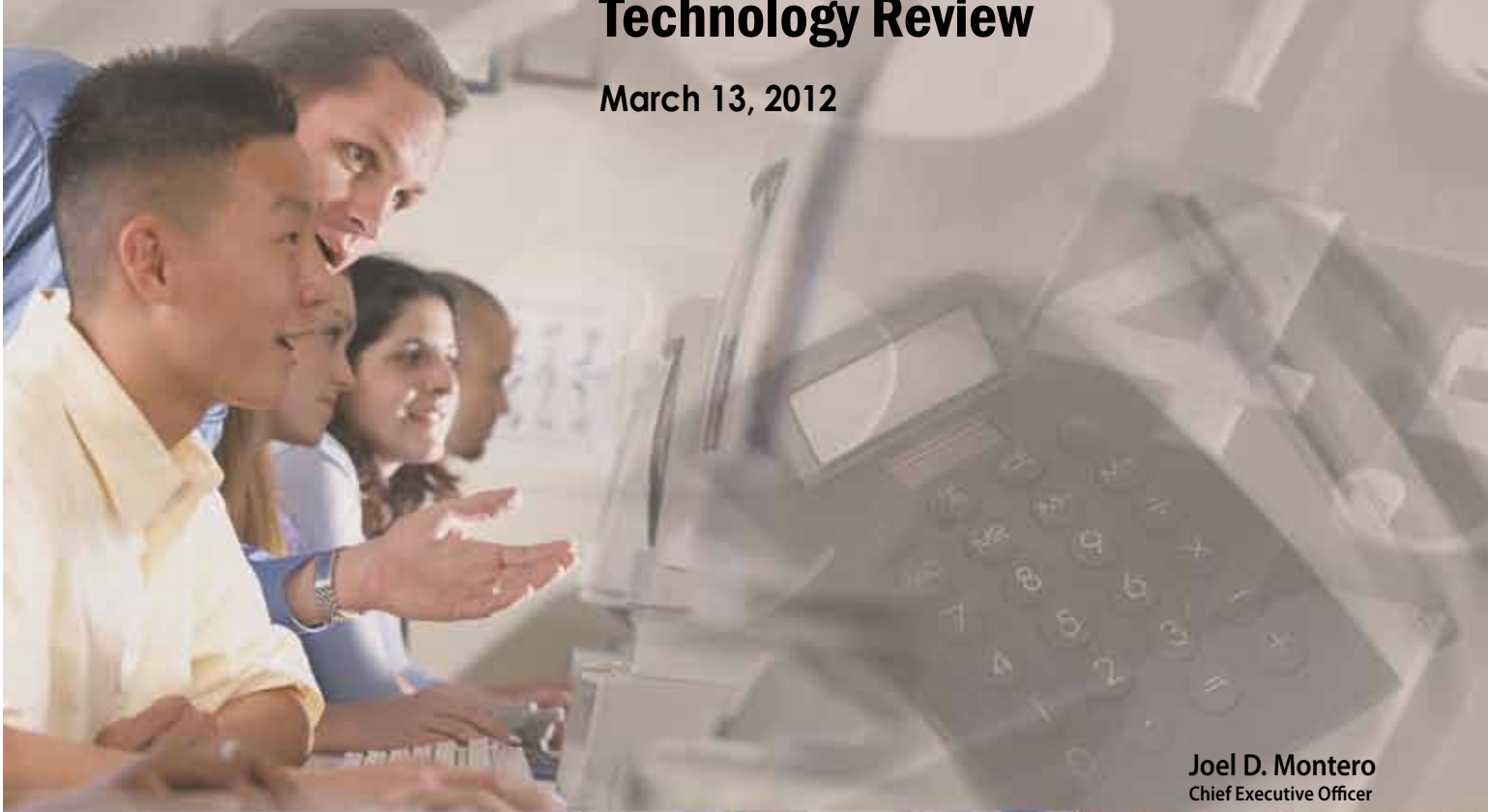


CSIS California School Information Services

Sanger Unified School District

Technology Review

March 13, 2012



Joel D. Montero
Chief Executive Officer







CSIS California School Information Services

March 13, 2012

Marcus P. Johnson, Superintendent
Sanger Unified School District
1905 Seventh Street
Sanger, CA 93657

Dear Superintendent Johnson:

In September 2011, the Sanger Unified School District and the Fiscal Crisis and Management Assistance Team (FCMAT) entered into an agreement for a technology review. Specifically, the agreement stated that FCMAT would perform the following:

1. Review the delivery of instructional and administrative technology services and make recommendations for improvement which shall include but not be limited to:
 - Website development and support
 - E-mail support for all staff including the district's archive and retention policy
 - Student attendance system
 - Technology equipment replacement plan
 - Evaluate board policies
2. Review the district's organizational structure for technology support services and make recommendations for improvement.
3. Review the district's staffing for technology support services and make recommendations for improvement.
4. Review the district's computer network administration and make recommendations for improvement.
5. Conduct an information assurance audit to review the security and privacy of district information and make recommendations for improvement.

FCMAT

Joel D. Montero, Chief Executive Officer

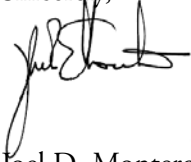
1300 17th Street - CITY CENTRE, Bakersfield, CA 93301-4533 • Telephone 661-636-4611 • Fax 661-636-4647

422 Petaluma Blvd North, Suite. C, Petaluma, CA 94952 • Telephone: 707-775-2850 • Fax: 707-775-2854 • www.fcmat.org

Administrative Agent: Christine L. Frazier - Office of Kern County Superintendent of Schools

This final report contains the study team's findings and recommendations in the above areas of review. We appreciate the opportunity to serve the [district name], and extend our thanks to all the staff for their assistance during fieldwork.

Sincerely,

A handwritten signature in black ink, appearing to read "Joel D. Montero". The signature is fluid and cursive, with a prominent initial "J" and "M".

Joel D. Montero
Chief Executive Officer

Table of contents

About FCMAT	iii
Introduction	1
Background.....	1
Study Guidelines	1
Study Team.....	2
Executive Summary.....	3
Findings and Recommendations.....	5
Role of Technology.....	5
Delivery of Services	7
Organizational Structure and Staffing	17
Network Administration	19
Appendices.....	23

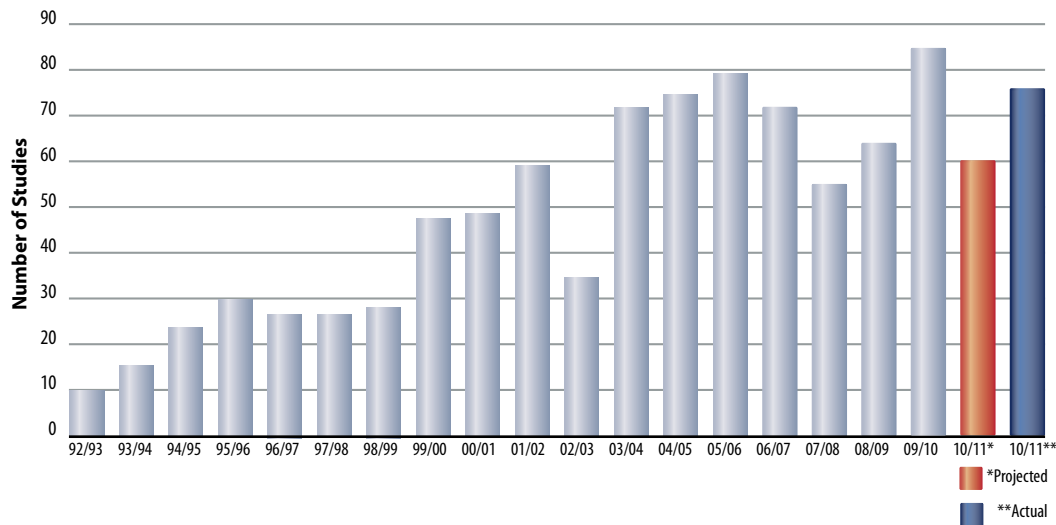
About FCMAT

FCMAT’s primary mission is to assist California’s local K-14 educational agencies to identify, prevent, and resolve financial and data management challenges. FCMAT provides fiscal and data management assistance, professional development training, product development and other related school business and data services. FCMAT’s fiscal and management assistance services are used not just to help avert fiscal crisis, but to promote sound financial practices and efficient operations. FCMAT’s data management services are used to help local educational agencies (LEAs) meet state reporting responsibilities, improve data quality, and share information.

FCMAT may be requested to provide fiscal crisis or management assistance by a school district, charter school, community college, county office of education, the state Superintendent of Public Instruction, or the Legislature.

When a request or assignment is received, FCMAT assembles a study team that works closely with the local education agency to define the scope of work, conduct on-site fieldwork and provide a written report with findings and recommendations to help resolve issues, overcome challenges and plan for the future.

Studies by Fiscal Year



FCMAT also develops and provides numerous publications, software tools, workshops and professional development opportunities to help local educational agencies operate more effectively and fulfill their fiscal oversight and data management responsibilities. The California School Information Services (CSIS) arm of FCMAT assists the California Department of Education with the implementation of the California Longitudinal Pupil Achievement Data System (CALPADS) and also maintains DataGate, the FCMAT/CSIS software LEAs use for CSIS services. FCMAT was created by Assembly Bill 1200 in 1992 to assist LEAs to meet and sustain their financial obligations. Assembly Bill 107 in 1997 charged FCMAT with responsibility for CSIS and its statewide data management work. Assembly Bill 1115 in 1999 codified CSIS’ mission.

AB 1200 is also a statewide plan for county office of education and school districts to work together locally to improve fiscal procedures and accountability standards. Assembly Bill 2756 (2004) provides specific responsibilities to FCMAT with regard to districts that have received emergency state loans.

In January 2006, SB 430 (charter schools) and AB 1366 (community colleges) became law and expanded FCMAT's services to those types of LEAs.

Since 1992, FCMAT has been engaged to perform nearly 850 reviews for LEAs, including school districts, county offices of education, charter schools and community colleges. The Kern County Superintendent of Schools is the administrative agent for FCMAT. The team is led by 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.

Introduction

Background

The Sanger Unified School District is located in southeast Fresno County. The district has an enrollment of approximately 10,800 students and serves the city of Sanger and the surrounding communities of Centerville, Del Rey, Fairmont, Lone Star, Tivy Valley and portions of the Sunnyside area of metropolitan Fresno. Encompassing about 180 square miles, the district has 19 school sites including three charter schools, a community day school, and an adult school.

On September 14, 2011, FCMAT and the Sanger Unified School District entered into a study agreement with the following scope and objectives:

1. Review the delivery of instructional and administrative technology services and make recommendations for improvement which shall include but not be limited to:
 - Website development and support
 - E-mail support for all staff including the district's archive and retention policy
 - Student attendance system
 - Technology equipment replacement plan
 - Evaluate board policies
2. Review the district's organizational structure for technology support services and make recommendations for improvement.
3. Review the district's staffing for technology support services and make recommendations for improvement.
4. Review the district's computer network administration and make recommendations for improvement.
5. Conduct an Information Assurance audit to review the security and privacy of district information and make recommendations for improvement.

Study Guidelines

FCMAT visited the district on October 31 and November 1, 2011 to conduct interviews, collect data and review documents. This report is the result of those activities and is divided into the following sections:

- Executive Summary
- Role of Technology
- Delivery of Services
- Organizational Structure and Staffing
- Network Administration
- Appendices

Study Team

The study team was composed of the following members:

John F. Von Flue
FCMAT Fiscal Intervention Specialist
Bakersfield, California

Andrea Bennett
A. Bennett Consulting
Claremont, California

Greg Lindner*
Director of Technology Services
Elk Grove Unified School District
Elk Grove, California

Andrew Schwab*
IT Director
Le Grand UHSD
Merced, California

Laura Haywood
FCMAT Technical Writer
Bakersfield, California

*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 Sanger USD Technology Support Services department provides support for all technology utilized in the district. The department has overseen the implementation of several infrastructure projects with assistance from the county office of education that have established a solid foundation on which to provide technology services. During interviews, the department received favorable feedback from users at all levels of the district.

Although district leadership and staff recognize the importance of technology's role in the district, technology needs are not always considered in decision making. Technology does not have direct representation at administrative meetings and is not always consulted when facilities and instructional decisions are made that require technology support. In addition, the technology plan required by board policy is not regularly referenced or updated to reflect changing district priorities.

Most staff interviewed reported that the services provided by the technology department are good and that the technology staff is knowledgeable and service oriented. However, the delivery of some services could be improved. Support ticketing is done through a work order system, but the system is not used consistently. Several essential processes in the department such as data backups are not supported by documented procedures or plans. The support staff's organization and function should be improved to provide more timely assistance when and where support is needed. Some skill sets and training opportunities are lacking, and job descriptions do not all align with actual responsibilities. Improved communications would provide technology staff with a better understanding of district needs and would keep technology users aware of how the Technology Support Services department can assist them.

Technology purchases are decentralized, with school sites and departments maintaining their own budgets for technology. The district has no defined standardization policies for the purchase or replacement of technology equipment, but Technology Support Services is responsible for the installation, maintenance and support of the equipment.

While most student data is kept in the district's student information system, some data is kept in separate databases within sites or programs. Data archiving is decentralized, with numerous employees responsible for backups and Technology Support Services providing little oversight. This results in extra staff involvement and effort to manage student accounts, business processes, and technology access. These operations would benefit from more centralized regulation of processes and training.

Findings and Recommendations

Role of Technology

The role of technology in education is far-reaching and has expanded significantly in recent years. Traditional administrative systems such as e-mail and websites may be high-visibility examples, but they represent a fraction of the technology assets that districts must maintain. Many school district technology networks serve as the backbone for phone systems, alarms, clocks, lights, digital signage, security cameras and other systems. The responsibility for maintaining these systems commonly falls to the technology department.

Assessing technology needs, involving stakeholders, developing a technology plan, investigating emerging technology trends, and designing sustainable models are all important aspects of an optimally functioning technology department. For technology implementation to be successful, staff members must maintain control over information security, the network infrastructure, and user support while keeping pace with the increasing demand for technology-enriched instructional programs. These demands increase the need for the technology leader in the organization to be engaged in all decisions that affect technology so the effect on the technology resources can be evaluated. The technology leader must have vision, good communication skills and access to resources and information that can help make necessary research efficient and effective.

Technology staff should have consistent and direct involvement in district decision-making processes, especially regarding facilities and instruction, to ensure technology needs and compatibility are considered. The technology department should have direct contact with district staff through regular, organized meetings to determine the needs of departments and sites, and to communicate technology advancements, limitations, and recommendations.

The district's Technology Support Services department does not have a direct role in district decision making. The department reports to the associate superintendent of business services through the director of technology services. Technology representation is not regularly included in facility planning meetings and, as a result, during recent modernization projects data and power cable drops were placed without consideration for technology use. The drops subsequently had to be routed to usable locations, which caused delay and additional expense to the project.

Decisions regarding technology are made by school site and department staff with varying levels of input from Technology Support Services. Technology staff members are accessible and provide help and recommendations when requested. However, no regular meetings are scheduled between technology and site staff to discuss technology purchases and services. Purchase orders for technology purchases are reviewed by the director of technology services, but this position has no control or authority to change or refuse a purchase. Issues regarding installation, upgrades, training and ongoing maintenance can occur if the technology procured does not align with the district's existing support and infrastructure. Coordination of technology purchases and implementation with sites and departments can result in increased purchasing power and greater support efficiencies.

The district does not have an active technology committee. The function of a technology committee is to discuss and coordinate technology purposes, review and update the district's technology plan, and help create the vision for technology use district-wide.

Technology Plan

Board Policy 0440 requires the development of a plan to address the technology needs of the district. The technology plan for Sanger USD covers the period of July 1, 2010 through June 30, 2015. Its vision statement indicates that all students and staff will have access to and use technology as a tool and resource. This plan should be accessible and regularly referenced for technology procurement, implementation, training, and use. It should also serve as a guide to support consistency and adequacy of district technology. Interviews of staff showed that the plan is rarely referenced. Few staff outside of the technology department and district administration are aware that the plan exists.

Financial Support

For fiscal year 2011-12, the district has budgeted approximately \$1,268,000 to support technology. Of that amount, approximately \$987,000 is budgeted to be spent on technology staff salaries, \$216,000 on supplies and software, and \$65,000 on operating expenses. While the budget for salaries is comparable to prior year expenditures, no budget was established for computer equipment for the current year, although approximately \$850,000 was spent in 2009-10 and \$45,000 was spent in 2010-11. The technology plan estimates equipment needs at \$68,836 in the current year.

Education funding in California has undergone a series of cuts over the last few years as the state attempts to respond to diminishing revenues and a budget imbalance. These cuts have forced districts, including Sanger USD, to reduce spending in all areas of their budget including technology. However, the district budget should reflect the allocation of funds to follow the district plan, including the consistent implementation of technology and support of the district technology needs as defined by the technology plan. Inadequate technology funding will lead to a lack of available support personnel, aged equipment, and inconsistencies in the delivery of technology services.

Recommendations

The district should:

1. Ensure that Technology Support Services is consulted and has representation in the decisions that may involve technology, including facilities construction and modernization projects, instructional hardware and programs, and data and communications systems.
2. Create a Technology Committee chaired by the director of technology, with members representing each school site and department.
3. Hold regular Technology Committee meetings. Encourage attendance and participation from all sites and departments. Distribute meeting minutes to site and department heads, including discussions, recommendations, and decisions.
4. Communicate and follow the adopted Technology Plan. Update the plan as needed to reflect changing district needs and goals, and post it on the department web page to ease accessibility.
5. Budget adequate funds to support the current and ongoing technology needs of the district. Should funding not be available, evaluate and adjust the technology plan.

Delivery of Services

Website Development and Support

Current Websites

All of the district's schools including 14 elementary schools, a middle school, a K-12 school, a comprehensive high school, an independent study high school, a community day school and an adult education school have websites. In addition, district departments have pages on the district's website. The links to the schools' websites are all formatted the same way, www.school-name.sanger.k12.ca.us, making it easy for people to locate and remember. All of the websites are also accessible through the district's main website.

The main tabs of the district's website show ED Services, Human Resources (HR), Business Services and a Parents tab. The format to access these sub sites is www.sanger.k12.ca.us/Department. Each tab has additional sub tabs to access the different areas in each department. There is no consistency of the information available at the sub tab level. For example, each department page should contain staff and contact information such as name, position, phone number and email. The development of content varies significantly, with some pages containing no information.

Technology Support Services Website

The Technology website is located under the Business Services tab. This website contains only the names, titles and phone numbers of each staff member, but there is no information on what products or services are supported or the area of support provided by each staff member. A fully developed website should serve as an information and reference source and should contain information such as district technology standards, technology policies, and training schedules.

Website Support

All websites are created and maintained in the First Class Web hosting service. A teacher on special assignment supports the websites. The websites are set up to allow school and department site personnel to add and change their own content. Each school and department can choose the font and colors, but the basic format of the sites is standardized and consistent throughout the district. This eliminates the need for a district webmaster position and allows subject matter experts to update the online information in a timely manner.

The district has not defined standards for website content, development, or maintenance. Some schools have one individual who is responsible for the website while other schools rotate the responsibility. The teacher on special assignment is responsible for monitoring district websites for appropriateness and provides training and assistance to individuals at the schools when needed. The position also provides support for the departments' content and verifies that all links are working properly. Because website support is assigned to various staff by site and department and the assigned staff have varying degrees of capabilities and expectations, there is no consistency in content or routine process to keep the content current. Having a job description for this role would serve to establish minimum qualifications and set expectations for the website support.

The district does not have a job description that identifies the responsibilities and requirements for the person maintaining the websites. Currently, the network specialist is responsible for the network and the accessibility of the websites. The network specialist and the teacher on special assignment work well together to ensure the sites are available and working properly.

Recommendations

The district should:

1. Create a job description for the district staff member responsible for the websites.
2. Post all district technology policies on the Technology website.
3. Post all products and services supported by Technology Support Services on the Technology website, and include the appropriate contact information for support of each product or service.
4. Post all training materials for supported technology products and services to the Technology website for staff reference.
5. Develop a standard describing the basic information required for each of the district's website pages. Update all pages with the information. Establish a template/style page for each school's and department's initial landing page to provide a consistent look and feel for all pages. Subsequent pages can then be more customized to the tastes of individual schools and departments.

Email

The district archives email but does not have a formal e-retention policy that defines retention times or communicates retention guidelines to users. At a minimum, a policy that documents current practices of server space constraints, retention lengths (30, 60, 90 days) and data recovery should be developed. If desired, the district may choose to develop a more formal policy that clearly identifies and communicates the different types of electronic communication (transitory vs. lasting value), what happens to electronic communication as it exists in the system and the responsibilities of users and technology staff with regard to the different types of electronic communication.

Recommendations

The district should:

1. Develop a retention policy for email, ensure all staff are aware of the policy, and implement procedures to enforce the policy.

Business Services

Sites receive a monthly budget update via email. This report is updated each month by the district business department and provides sites and departments with an overview of their current budget and expenditures. The sites and departments keep separate spreadsheets in the interim to track their expenditures and balances.

Purchase requests are not handled electronically. The information for the purchase is sent to the district office by hard copy, fax, or email. The business department staff then generate a purchase order.

Providing sites and administrators online access to the district's financial system to review their budgets, track their expenses in real time, and input their own purchase requests would reduce work for the business office and the additional record-keeping required at the sites/departments, and increase the availability and timeliness of information.

Recommendations

The district should:

1. Provide key site and department personnel access to and training on the district's financial system so they can initiate purchases and query their budget information and reports.

Student Information System

Student enrollment and attendance data resides in the district's student information system, PowerSchool, which is a Web-based system supported by Pearson School Systems. All schools in the district use PowerSchool for attendance reporting. Student information such as grades, schedules and demographics is also kept in PowerSchool.

Setup

PowerSchool is user account and password based. Technology Support Services is responsible for the setup and maintenance of the user records in PowerSchool. Each individual granted an account is given access to the data based on their job function. New users are given accounts and passwords based on information obtained by the HR department or by the school's administration. New users are required to sign the district's Acceptable Use Policy (AUP) before a password is issued. While this process has recently improved, in some instances staff accounts are set up at the request of a site without going through HR first. Accounts and passwords are given even if the new user has not been trained.

Technology Support Services sets up the parameters in PowerSchool based on the school calendar adopted by the school board. The department also sets up and maintains the attendance codes, bell schedules, entry and exit codes and special program attendance accounting requirements.

Training

Technology Support Services provides documentation to users for PowerSchool and is responsible for training new users on attendance procedures in the software. Department staff developed documentation specific to the procedures at Sanger Unified. However, no routine training schedules are developed during the school year. Information regarding new users is received by the Human Resources office and training needs are determined by Technology Support Services. New information regarding attendance procedures is communicated through the district's email system. While teachers receive attendance training at the beginning of the year, classified staff hired during the year do not receive any formal training. Only one person in Technology Support Services that supports the system has been formally trained.

The lack of properly trained staff can lead to inaccurate and incomplete information being entered into the PowerSchool system, which will cause confusion, added workload during state reporting and possible financial implications if the enrollment or attendance data is wrong. Training needs include but are not limited to log-in procedures, the importance of password privacy, student record confidentiality, and how to access data.

Data Entry and Reporting

Teachers enter student attendance information into PowerSchool from their classroom computer. Attendance clerks at each school are responsible for verifying attendance data. The clerks also are responsible for the weekly and monthly attendance reports. These reports are sent to the Child Welfare and Attendance Department at the district office. This department is responsible for attendance reporting to the state of California. Technology Support Services is responsible for troubleshooting all attendance issues.

Overall, data in PowerSchool appears to be handled well. Interviews indicated that there were few issues with the system and that data is entered consistently throughout the schools. The system is set up district-wide with the appropriate state and federal required codes.

Inconsistencies have occurred in the past with the implementation of district data input policies, which has created issues. For example, some schools were told to leave students active in the system until a cumulative folder was requested, even though they no longer resided or attended school in the district. This was inconsistent with past practice and resulted in problems with state data reports.

Some departments maintain data outside of PowerSchool in their own databases. This creates the need for double entry of data and/or can create problems with CALPADS and CBEDS reporting. In addition, information is not readily accessible as desired by the district office, departments and programs.

Many student data queries are made to the sites by departments and other sites. Because these queries are made to numerous sites, the employee responding varies. This results in inconsistent queries and reporting. With the data all available in the district PowerSchool database, the queries should be centralized for efficiency and accuracy.

Substitutes

There are no standard procedures for training substitutes in the schools' attendance offices. The schools are responsible for acquiring substitute clerks when needed and the school's clerk is responsible for training the substitute on the PowerSchool procedures.

Recommendations

The district should:

1. Establish a formal, written Acceptable Use Policy process so no one gets a logon for PowerSchool without a signed AUP on file. Require all requests for account creation to come from HR and to include the signed AUP before the account is created.
2. Provide regular, formal training as needed for new clerks in the correct use of the PowerSchool software. Establish required training for new employees prior to giving them access to PowerSchool.
3. Seek extensive PowerSchool training for at least two to three district employees through PowerSchool University.
4. Establish a policy to route data extract requests through Technology Support Services before asking sites for the data. Have Technology Support Services complete the PowerSchool queries. Implement a procedure to have all data requests reviewed by the division head and routed to Technology Support Services for possible extraction prior to sending to school sites.
5. Work with various district departments to minimize student data retention outside of the PowerSchool software and to ensure consistent and timely input of data into PowerSchool.
6. Develop training for all substitutes on PowerSchool via an online video as well as requiring they sign the AUP. Provide substitutes with temporary logon accounts that are suspended when the substitute is not working.
7. Develop a district procedure for data input that ensures communication of the correct information.
8. Establish policy and procedures for providing substitutes with the appropriate training and access to the attendance system.

Technology Equipment Replacement Plan

Process

The district has developed a process for funding regular upgrades to E-Rate eligible network equipment utilizing priority one reimbursement funds as carryover from year to year. Priority one E-Rate items are funded first, prior to internal connections. With these funds, the district is able to upgrade core network services every five to six years. While the network infrastructure is refreshed on a district-funded schedule, sites determine local technology purchasing priorities, including desktop computers. Sites and departments set their own priorities and budgets for end user technology purchases. This has led to disparity among school sites in the technology provided to both teachers and students. By establishing a plan and funding to replace sites' end user computer hardware, the district can ensure uniform access to technology in the classroom in support of learning communities and district goals. In addition, there is no formal process for

review or authorization to ensure the technology aligns with district priorities and can be properly supported by district resources.

A list of current and recently purchased equipment should be utilized to start a standards list. That list should be accessible (posted on the Technology Support Services web page) along with the best available pricing. The list should be regularly updated as new requests for items not on the list gain volume (more people requesting them) and outdated items are no longer recommended.

Inventory

The district does not maintain a detailed inventory list of desktop and laptop computers and software currently in use. Although Education Code 35168 only requires that an inventory be maintained for equipment valued at more than \$500, more detailed information regarding technology in use is important to identify needs for current and future equity, stability, and compatibility. Interviews and on-site observations identified a disparity in the type, age, and condition of technology available to the end user. Identification of current holdings is one of the first steps in creating a comprehensive replacement plan. Without knowledge of the current inventory, it is very difficult for the district to assess maintenance and replacement needs and to develop a plan that addresses those needs.

Procurement Method

As stated above, end user technology hardware and software purchase decisions are made by individual sites and departments. The purchases are made out of their site/department funds and are based on local priorities and current budgets. The long term maintenance and replacement of end user devices is not generally considered.

Cost savings in both procurement and maintenance may be realized through the consolidation of purchases and a regular replacement plan. One such option is leasing. Leasing would ensure that the equipment replacement becomes an integral part of the budget process as opposed to using one-time funds as they become available. Over time, this will reduce equipment inequities among departments and sites. Leasing also makes it possible to upgrade more equipment for a given budget because the cost is spread out over multiple years. For districts with a large inventory of aging hardware, leasing is a cost effective means to jump start a replacement plan.

Both purchase and cumulative lease contracts are subject to Public Contract Code 20111, which requires school districts to competitively bid contracts for the purchase of equipment, materials, supplies, services, repairs, and maintenance if the amount is over \$81,000 (adjusted rate effective January 1, 2012 for other than public works or construction services). The bid process is required to help ensure that competitive pricing is obtained and that public funds are used optimally.

Recommendations

The district should:

1. Continue to maximize E-Rate eligible network equipment replacement and support.
2. Establish, maintain, and regularly communicate district minimum acceptable technology standards to ensure equitable resources to all staff and students.

3. Maintain an inventory of current technology hardware and software. Include a description, date purchased, how funded, current location, and a unique identification number to facilitate tracking.
4. Establish a formal process in which Technology Support Services evaluates technology purchases to ensure they are within district standards and the department is able to provide adequate support.
5. Review the costs of lease vs. purchase procurement methods based on district standards and replacement goals.

Policies

The district has a basic set of board policies related to technology that is consistent with many districts of comparable size. The policies address acceptable technology purpose and use in the district and, in most cases, serve to meet the needs of the district.

Board Policy and Administrative Regulation 4040 are outdated and insufficient. BP 4040 contains the following statement:

When passwords are used, they must be known to the Superintendent or designee so that he/she may have system access.

The superintendent or their designee can gain access to accounts without knowing the password. Best practices discourage the sharing of passwords. This clause could cause confusion among employees in communicating a safe password policy. In addition, AR 4040 does not provide enough information as to the safe handling of passwords. Language should be added specifying the importance of using strong passwords, not sharing passwords or logon information with anyone. The proper handling of confidential data should also be addressed.

Sample policies are provided as Appendix B for reference.

Recommendations

The district should:

1. Regularly review and update board policies to ensure they are consistent with federal, state, and local law and meet district needs.
2. Amend BP 4040 to remove the requirement that the Superintendent or designee know user passwords.
3. Update AR 4040 to include information on password, logon and confidential information safety (see sample provided in appendices).

Help Desk

Technology Support Services uses the free MyTechDesk help desk ticketing system obtained from the Imperial County Office of Education. The network specialist is responsible for reviewing and assigning the trouble tickets submitted through the help desk system. During interviews,

several individuals said that they did not use MyTechDesk and instead chose to directly call the person that could help them. Going outside the ticket queue for support impacts the department's ability to manage support issues, balance the requests appropriately, and identify potential trending issues that require higher level investigation. Furthermore, the Maintenance and Operations department uses a different ticketing system, SchoolDude. This means end users must know and use two systems for requesting help. Certain ticket systems have the added benefit of an automated asset management system for technology, which would provide the department with information regarding the type and frequency of repairs on all equipment. These systems also can provide an up-to-date inventory of desktop hardware and software, which the district was not able to provide during the site visit.

Recommendations

The district should:

1. Evaluate current help desk systems and consider standardizing to a single ticketing system district-wide.
2. Consider implementing a help desk phone number with dedicated staff to answer and provide level 1 support and to route tickets, thus alleviating this responsibility from the network specialist.
3. Require all technology issues to be documented through the help desk ticketing system to develop a knowledge base of frequent and/or reoccurring issues and trends.

E-Rate

The director of technology estimated that he spends up to two months per year working on E-Rate related responsibilities. Applying for and complying with E-Rate regulations can be complex and time consuming. Ensuring proper document retention and audit requirements are met and keeping up with rule changes from year to year all contribute to the amount of time required to secure funding. Districts of various sizes often choose to outsource maintenance of the E-Rate application, paperwork and audit response to consultants in an effort to ensure current E-rate expertise, economize resources, and allow district staff to focus on internal operations. Contracting out the day-to-day paperwork management can help reduce the staff workload and allow Technology Support Services to focus on servicing customers. Many districts fund E-Rate consultants with a percentage of savings from priority one reimbursements.

Recommendations

The district should:

1. Consider the cost/benefit of engaging a consultant to partially or fully handle E-Rate application and auditing paperwork.

In-House Repairs

Computers are repaired by Technology Support Services. This may not be the most efficient means of servicing the district's technology support needs. However, the district does not currently identify and track costs associated with in-house repairs. Technology staff must maintain expertise on the various types of equipment in service. Technology Support Services does not maintain a spare parts inventory. The repair parts are approved, ordered, and charged to the applicable site or department. Repair turnaround times of up to three days can occur while waiting for purchase order approvals and shipping. This also requires the district to go through the purchasing process for each item needed.

Common parts such as laptop hard drives could be stocked and replacements ordered to shorten the turnaround time for service and consolidate purchasing. Record-keeping in Technology Support Services could still allow sites and departments to be charged for the repair costs.

Recommendations

The district should:

1. Establish an inventory of common spare parts to reduce service repair times.
2. Establish a system to invoice sites and departments for repairs.
3. Identify the costs associated with personnel, labor, training, and time away from other tasks. Subject to bargaining agreement limitations, consider outsourcing the repair and maintenance of equipment that would be more cost effectively and efficiently performed by outside sources.
4. Consider including manufacturer extended service and/or maintenance agreements when purchasing equipment.

Organizational Structure and Staffing

Technology Support Services reports to the associate superintendent of business services.

Technology Support Services consists of a director of technology support services to whom the following positions report: secretary II, information systems manager, network specialist, database administrator, technical support analyst, staff support specialist, telecommunications support specialist and four technical support specialist I positions. The department does not have current organizational chart, and many job descriptions for the department are in draft form.

Interviews and observations revealed the following staff roles and duties:

The director of technology support services is responsible for the effective, appropriate and successful use of technology throughout the district. The director also is responsible for all E-Rate planning, application, and reporting for the district. This position reports to the associate superintendent and is not part of the superintendent's cabinet or executive committee and does not meet regularly with principals.

The secretary II position performs administrative support duties for the department. This position reports to the director of technology support services.

The information systems manager handles student data and state reporting through CALPADS. This position works directly with the database administrator and the technical support analyst to analyze, correct and report data to the district, county and state. This position does not support business or other systems, websites or the network. No consistent training is provided for this position, although technology staff do communicate regularly with the California Department of Education and California School Information Services (CSIS) for information on data requirements.

The network specialist supports the hardware and software required for the district's network and access to the Internet. This position also supports the district's online communication system called First Class, which includes email, calendars, file sharing and online collaboration. This position works closely with the Fresno County Office of Education to troubleshoot and improve the district's Internet access and internal network performance. The network specialist reviews and assigns the trouble tickets submitted through the district's work order system but does not supervise all of the positions to which tickets are assigned. This position works directly with the telecommunications support specialist.

The database administrator supports the Oracle database containing student information entered through PowerSchool. This position also enters additional student information necessary for state reporting that is currently held in other systems, and works directly with the information systems manager to ensure data is complete and correct.

The technical support analyst is responsible for all repairs and replacement of Apple computer equipment. This position works directly with the technical support specialists to receive, repair and return equipment to the district's schools and departments. This staff member also supports the setup and users of the First Class system. This position assists with data correction and obtaining statewide student identification numbers, working directly with the information systems manager and database administrator. The technical support analyst also assists with creating user accounts for PowerSchool and provides end user support, mostly via phone.

The staff support specialist provides end user support for the First Class system, including the websites. This position works directly with the HR department for new accounts including ensuring the Acceptable Use Policy has been signed. The staff support specialist checks the

district's websites for appropriate content and contacts the staff responsible when changes are needed.

The telecommunications support specialist maintains the telephone and data communications systems. This includes the installation, removal and location changes of equipment, and working with the Fresno County Office of Education to ensure the district's communication systems are working properly. This position works directly with the network specialist.

The four technical support specialist I positions support all personal computers in the district, both Apple and PC computers. These positions provide on-site and phone support for the installation, setup and repair of the computers, with each specialist supporting multiple sites and one position supporting the district office. Specialists spend substantial time repairing aged computers because the district has no technology equipment replacement policy.

FCMAT found that no consistent training is provided for most positions in the department to ensure that staff are current on the latest technology developments and are able to provide hardware, software, and user support.

Recommendations

The district should:

1. Create and regularly update an organizational chart for the department to identify current lines of responsibility and relationships between positions.
2. Complete and present the department job descriptions to the personnel commission for approval.
3. Modify technical support positions' job descriptions to accurately identify the duties for which they are responsible.
4. Reassign duties as necessary to ensure that technology staff members' duties appropriately reflect the job description identified with the job title.
5. Regularly evaluate the duties being performed by technology staff to ensure that workload, capabilities and district needs align with staff responsibilities.
6. Evaluate the need for and provide regular trainings that align with staff responsibilities. This should include online training opportunities that provide specific professional development at lower costs than on-site training.
7. Establish a training plan for each position and then budget for both online and in-class studies to help provide for the needed technical skills for all technology department staff.
8. Set standards for data quality and enforce the standards at all levels of data handling.
9. Develop and implement a district plan for professional development for technology users.

Network Administration

Systems Management

The district has recently deployed an Apple-recommended configuration that links Open Directory and Active Directory and allows the cross-assignment of users and resource permissions between the two directory systems. For mixed Windows and Mac environments, it is a good way to integrate services and reduce support time. However, it was noted during the site technician interviews that Windows server administration skills are primarily self-taught through trial and error and on-the-job experience. Common Windows management tools such as Group Policy and Windows Server Update Services are not in use. These tools allow for streamlined support. Proper configuration and use of these tools provides regular security and system updates. Staff need to be well versed in the support and management of Windows servers and clients to ensure a secure and stable end user experience.

The district has deployed directory service at the school sites to store student accounts; however, the directories do not talk to one another. As students matriculate through the district, their accounts must be re-created at each site. While this approach is straightforward, there are benefits to having a unified directory structure that includes all accounts:

- Student accounts need only be created once.
- Only exiting students' accounts must be purged.
- Student electronic files can follow the student through to graduation.
- Centralized account management.

Recommendations

The district should:

1. Provide support staff training on proper Windows system management and administration.
2. Conduct a review of the network directory architecture and consider unifying site directories into a single, global directory for centralized account management.

Connectivity

Network

Technology Support Services does not know how much bandwidth is utilized between sites. Visibility into the network is a critical factor in determining future bandwidth needs or diagnosing network issues due to bottlenecks. It is also a factor in determining the capacity to centralize services away from the local sites to streamline service and support. The county monitors the Internet connection, but a system to monitor site-to-site and local area network (LAN) traffic will improve decision making and network troubleshooting.

School Sites

After reviewing network topology documents, FCMAT determined that each school site is allocated a class C subnet for the wireless network. A class C subnet represents 254 available network addresses. With the rise of mobility and wireless devices, the district should consider how many wireless devices it plans to support. Many districts plan to accommodate two to three wireless enabled devices per person (student and staff) on campuses in the near future and are building their infrastructure accordingly. Expanding the available internet provider (IP) addresses for wireless access should be considered if the district decides to pursue increased staff and student access to wireless devices such as smart phones, tablet computers, and laptops.

Recommendations

The district should:

1. Implement a network monitoring solution such as The Dude (free), CiscoWorks LAN Management (paid) or Solarwinds Network Performance Monitor (paid) to track bandwidth utilization, communications latency and system availability.
2. Evaluate wireless access needs and consider expanding available IP addresses in wireless subnets.

Hardware Maintenance

During FCMAT's site visits, it was noted that the Networks Operations Center server room was warm. Heat can be a problem, especially if not monitored and allowed to reach critical temperatures. High temperatures can bring systems down and reduce the life spans of hard drives. A device to monitor and send alerts when temperatures reach critical levels is an inexpensive and proactive step that can prevent more serious problems. Several options exist: Tripp Lite, the maker of the district's UPS units, has a temperature monitor called Envirosense. Third parties such as Sensaphone make standalone units.

In addition, two servers were observed with flashing orange event lights indicating a failure or warning of some kind. The department does not have a centralized monitoring application in place to identify and alert support personnel to potential hardware failures. With servers located at each site and site techs not on site every day, potential failures must be identified as quickly as possible to prevent down time. A hardware monitoring and notification system such as Nagios or The Dude would address this.

Recommendations

The district should:

1. Install a temperature monitoring device with alerting capabilities in the Network Operations Center.
2. Install a hardware monitoring application to monitor and alert on server hardware failures.

Backups

Data protection is a critical role for technology departments. While the district backs up critical servers and some site servers, individual site technicians are each responsible for maintaining backups for the servers they support. The department does not have a centralized backup with reporting and monitoring in place for servers. This means that the Technology Support Services management cannot see the state of backups across the district at any given time. Without a monitoring and reporting system in place, there is no way to know whether backups were successful without manually checking each system. This can be time-consuming.

The district does not have a formal backup policy or plan in place to ensure data is properly backed up. The backup routines and schedules should be documented in a backup plan, and a policy should be developed. The backup policy should include what needs to be backed up and how often, who is responsible for the backup, how they will ensure the backup is completed, and what the procedure is for restoring in the event of data loss. The policy should correspond with a backup plan that outlines the measures taken to ensure data protection per policy requirements and addresses disaster recovery in the event of a catastrophic data loss.

Interviews indicated that the department relies heavily on one network engineer at the county office of education for higher level network and voice over IP (VoIP) system support. While maintaining a close working relationship and supplementing key skills with outsourced support are acceptable strategies, the district should consider developing in-house knowledge to provide backup support with the eventual possibility of providing more network and VoIP system administration support within the department.

Recommendations

The district should:

1. Document backup procedures and enable notifications in current systems.
2. Develop and implement a backup policy and plan to ensure that all data is uniformly archived.
3. Identify backup needs and evaluate potential centralized solutions that can provide reporting and notification for backup events.
4. Develop Cisco networking and VoIP skills (Cisco certified network administrator, Cisco certified network professional training) for department staff.

Security and Privacy

Wireless

Wireless security in the district is very strong using Media Access Control (MAC) addresses, meaning that each laptop is manually given access via its MAC address. This ensures no unauthorized laptops are allowed on the network. However, secure alternatives to managing wireless device access exist that the district might consider as more wireless devices are deployed, since controlling access at the MAC level is a manual process. Integrating wireless access with user

network accounts using a tool like RADIUS authentication would allow users to sign in to access the wireless network without the technology department first having to physically handle the device. Several schools that are deploying bring your own device programs, allowing visiting and roaming users with permission to securely access the district network, have taken this approach. RADIUS support is built into most wireless equipment.

Passwords

The district has no process or policy regarding changing or updating passwords. Passwords are not required to be changed regularly. Passwords issued for PowerSchool do not expire, and some PowerSchool user passwords have not been changed in more than five years. This increases the chances of passwords being compromised and/or the system being accessed by unauthorized personnel, and opens a window for hacking the various systems.

Passwords should be set to automatically expire and force a reset in all systems that have that functionality. Those without the functionality should be done via an email notification to users to change their passwords within a specified period.

Recommendations

The district should:

1. Consider implementing an authentication tool that will streamline accessibility while maintaining wireless security.
2. Develop and implement policy and procedures for periodic password change, maintenance, and updating.

Appendices

Appendix A

Study Agreement

Appendix B

Sample Policies and Procedures

Appendix A

FCMAT

FISCAL CRISIS & MANAGEMENT
ASSISTANCE TEAM

CSIS California School Information Services

**FISCAL CRISIS & MANAGEMENT ASSISTANCE TEAM
STUDY AGREEMENT
September 1, 2011**

The FISCAL CRISIS AND MANAGEMENT ASSISTANCE TEAM (FCMAT), hereinafter referred to as the Team, and the Sanger 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 Sanger 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.

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. The final report will be published on the FCMAT website.

2. SCOPE OF THE WORK

A. Scope and Objectives of the Study

The scope and objectives of this study are to:

The District is requesting the FCMAT Team to conduct a comprehensive review of the technology department that will include the following components:

1. Review the delivery of instructional and administrative technology services and make recommendations for improvement which shall include but not be limited to:
 - Website development and support
 - E-mail support for all staff including the district's archive and retention policy

- Student attendance system
 - Technology equipment replacement plan
 - Evaluate board policies
2. Review the district's organizational structure for technology support services and make recommendations for improvement.
 3. Review the district's staffing for technology support services and make recommendations for improvement.
 4. Review the district's computer network administration and make recommendations for improvement.
 5. Conduct an Information Assurance audit to review the security and privacy of district information and make recommendations for improvement.

B. Services and Products to be Provided

Orientation Meeting - The Team will conduct an orientation session at the School District to brief District management and supervisory personnel on the procedures of the Team and on the purpose and schedule of the study.

On-site Review - The Team will conduct an on-site review at the District office and at school sites if necessary.

1. Exit Report - 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.
2. 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.
3. Draft Reports - Sufficient copies of a preliminary draft report will be delivered to the District administration for review and comment.
4. Final Report - Sufficient copies of the final study report will be delivered to the District administration following completion of the review.
5. Follow-Up Support – Six months after the completion of the study, FCMAT will return to the District, if requested, to confirm the District's progress in implementing the recommendations included in the report, at no cost. Status of the recommendations will be documented to the District in a FCMAT Management Letter.

3. PROJECT PERSONNEL

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

- | | |
|--------------------------------|---------------------------------------|
| <i>A. Anthony Bridges, CFE</i> | <i>FCMAT Deputy Executive Officer</i> |
| <i>B. To Be Determined</i> | <i>FCMAT Consultant</i> |
| <i>C. To Be Determined</i> | <i>FCMAT Consultant</i> |

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. 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.

Based on the elements noted in section 2 A, the total cost of the study is estimated at \$11,500.

- 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 or proposed organizational charts
 4. Current and two (2) prior years' audit reports
 5. Any documents requested on a supplemental listing
 6. Any documents requested on the supplemental listing should be provided to FCMAT in electronic format when possible.
 7. Documents that are only available in hard copy should be scanned by the district and sent to FCMAT in an electronic format.
 8. All documents should be provided in advance of field work and any delay in the receipt of the requested documentation may affect the start date of the project.
- 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 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:


<i>Orientation:</i>	<i>September 20, 2011</i>
<i>Staff Interviews:</i>	<i>to be determined</i>
<i>Exit Interviews:</i>	<i>to be determined</i>
<i>Preliminary Report Submitted:</i>	<i>to be determined</i>
<i>Final Report Submitted:</i>	<i>to be determined</i>
<i>Board Presentation:</i>	<i>to be determined</i>
<i>Follow-Up Support:</i>	<i>If requested</i>

7. CONTACT PERSONName of contact person: Eduardo MartinezTelephone: (559) 524-6521 FAX: (559) 875-1081E-Mail: Eduardo_martinez@sanger.k12.ca.us

Marcus P. Johnson, Superintendent
Sanger Unified School District

9-14-11

Date



Anthony L. Bridges, CFE
Deputy Executive Officer
Fiscal Crisis and Management Assistance Team

September 1, 2011

Date

Appendix B

AR 4040.1(a)

Personnel

EMPLOYEE USE OF EMAIL

By using the email system, the employee or user expressly consents to the District's email policy. The user agrees not to misuse or abuse the email system, agrees to comply with all limitations set forth for the use of the email system in this regulation and related District policies and regulations and understands that the email system is not a private communication medium.

Violation of these policies will be subject to administrative review and possible disciplinary action, up to and including dismissal, if deemed necessary.

Business Tool:

The email system is a business tool owned and paid for by the District; therefore, the email system is the District's property. All email messages are the property of the District and are subject to office policy, procedures and control. As such, the District has the right to review them at any time.

Spam:

Spam is defined as unwanted, non-business email either being sent into the District or sent by someone within the district. Messages of this nature can include chain letters, cartoons, etc. Employees should not send out spam emails.

The District will make every effort to ensure that email messages received in the spammail@egusd.net inbox are reviewed on a daily basis and that valid emails are unblocked and sent to the intended recipient.

Incoming spam will be processed in the following manner:

All email messages blocked as spam receive the following notification via reply email:

Your email message has been blocked as a possible Spam email by the EGUSD Mail Filtering System. If you feel your message is not spam mail and should have gone through unblocked, please forward the blocked message to spammail@egusd.net, and we will research your request in a timely manner. Thank you for your cooperation.

Email messages received in the spammail@egusd.net Inbox are reviewed on a daily basis. The requests for unblocking are forwarded to the intended recipients with the additional email text added:

Hello,

I wanted to verify that the email address below is a valid sender to you.

Thanks,

XXXXX XXXXXX

{SR050643.DOC}

AR 4040.1(b)

Email Administrator
EGUSD – Technology Services
xxxxxxx@egusd.net

Once confirmation is received back from the District staff member, the request for having the outside sender's email address added to the unblocked list is processed according to the response of the District staff member; positive verifications are added to the unblocked list, negative verifications are discarded. In cases where the staff member is unsure about the identity of the outside sender, the designated Technology Services staff member will attempt to provide any additional information that could be used to assist in the verification process, including forwarding the original, blocked email messages. With all requests received for unblocking email addresses, Technology Services will review the message content to ensure that the subject matter does not violate EGUSD District Standards for appropriate conduct.

In cases where an outside email address is positively identified as a valid sender, in addition to adding that address to the unblocked list, a notification is also sent out to the District staff member who verified the outside sender's identity and the outside sender confirming that the email address has been unblocked.

Technology Services will make all efforts to process requests for unblocking within 24 hours of receipt of the original, unblocking requests. The only exceptions to this are requests that are submitted either during the weekend or on any district-wide holiday. Those requests will be processed as quickly as possible with a goal of within 24 hours of the Technology Services staff members returning to regular business hours. It should also be noted that should the District recipient be unavailable or not respond to the email, it will extend the timeline.

District staff members can also submit requests for email unblocking directly to the spammail@egusd.net address using their internal, EGUSD email account. Because access to these email accounts is limited to verified District employees, no additional identity verification will be necessary in order to process these requests. Any specific email addresses indicated within these requests will be added to the unblocked list as quickly as possible with a goal of within 24 hours of their receipt. As the processes for filtering email for spam are updated or change, additional methods for requesting email addresses be unblocked will be made available to all staff members.

Phone requests for email addresses to be added to the unblocked list will not be processed under any circumstances. In addition, requests to have entire domains added to the unblocked list, i.e. gmail.com, ibm.com, dss.ca.gov, will not be added to the unblocked list due to the potential for increased spam entering the district due to spoofed email addresses. Only specific, individual, email addresses will be added to the unblocked list.

Parent Emails:

Email communication is a very effective means for parents to communicate with their student's teacher. Teachers and other District employees will make every effort to respond to parent emails in a timely manner.

{SR050643.DOC}

AR 4040.1(c)

To avoid the delay of parent to teacher emails, it is preferred that schools annually update email addresses in SISWEB as these are automatically added to the “unblocked” list. Otherwise there may be a delay for some parents getting their emails through to teachers.

Privacy of Email:

The District respects the individual privacy of its employees. However, this privacy does not extend to the employee's work-related conduct or to the use of District provided technical resources or supplies, including District provided Internet or email accounts. Therefore, employees have no right of privacy as to any information transmitted or stored through the District's email system. To ensure proper use, the District may monitor its technological resources at any time without advance notice or consent. Employees shall use the email system for purposes related to their employment with the District.

Review and Retention of Email:

The District will comply with all state and federal laws as well as District policies and regulations governing retention of email, including email which may be classified as business records, employee records or student records. The Districts current retention period for archival of emails is three years. After that time all emails will be permanently deleted.

The Technology Services Director (or designee in charge when the Director is out) will review email accounts as part of a requested investigation if a written (paper or email) request is received from any of the following individuals;

- Associate Superintendent of Human Resources
- Classified or Certificated Director of Human Resources
- Legal Compliance Specialist
- EGUSD Police Services Chief or Assistant Chief
- Technology Services Director
- Superintendent

Investigations typically are initiated due to an allegation of a violation of law or district policy.

If time is of the essence, a verbal/phoned request is acceptable from one of the individuals listed above. In such a case, a follow-up, confirming email should be sent to the requestor stating, “Technology Services is proceeding to facilitate the request received via person/phone”.

The purpose of this procedure is to insure that Technology Services always has an authorized request to review email and does not do so without proper authorization.

If both the Director and designee in charge are not available, the Email Administrator may review the request after confirming with the requestor that time is of the essence and they choose not to wait until these people’s return.

Often times, when an employee leaves the district, their manager will need access to the employee’s email to find information they need to conduct EGUSD business. These requests will normally be approved as standard business as long as a notification is also sent to the Director of Technology Services.

{SR050643.DOC}

Inappropriate Use of Email:

Use of the email system that promotes unethical practices, or any activity prohibited by law or District policy is strictly prohibited. Except as otherwise indicated in this policy, commercial or political use of the email system is also strictly prohibited. Messages relating to or in support of illegal activities are strictly prohibited and shall be reported to District authorities and may also be reported to legal authorities. Employees should be aware that computer files and communications over electronic networks, including email are not private. This technology should not be used to conduct personal commercial business or to express personal opinions or personal statements not related to the work at hand, as it is a limited forum and not a public forum.

User Responsibilities

The transmission of information about students or District affairs shall adhere to the following:

- Confidential information should never be sent or forwarded to outside individuals or outside agencies not authorized to receive that information.
- Confidential messages and information should never be sent or forwarded to others, including faculty, staff and students who do not need to know the information.
- Confidential information should not be forwarded to multiple parties unless there is a clear and legitimate need to do so.
- Confidential email should not be retained in an employee's personal mailbox, but should be deleted as soon as possible. Records that need to be kept should be printed and retained according to appropriate policy or regulation.
- Confidential messages from or to legal counsel should not be forwarded to others without counsel's authorization, since such messages may constitute privileged communications between the District and its attorney.

Confidential information includes, but is not limited to, "Personnel records, medical records, student records, or similar materials the disclosure of which would constitute an unwarranted invasion of personal privacy."

Acceptable Use

- Employees shall use the District's technology system, including District-provided email accounts, safely, responsibly, and primarily for work-related purposes.
- The employee in whose name an account is issued is responsible for its proper use at all times. Employees shall keep the account information, addresses, and telephone numbers of other employees private.
- Network accounts are to be used only by the authorized account holder.

AR 4040.1(e)

Prohibited Use

- Employees shall not access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race, ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion or political beliefs.
- Users shall not use email in ways that violate any copyright laws. This includes but is not limited to distribution of copyrighted information, graphics and software.
- Employees shall not send unnecessary messages to a large number of people (i.e. chain mail).
- Email shall not be used to produce, distribute, access, use or store information which would subject the District or the individual to criminal, civil or administrative liability for its use, production, distribution, access or storage.
- Employees shall not use the District's system to engage in commercial or other for-profit activities without the permission of the Superintendent or designee.
- Employees shall not use the system to promote unethical practices or any activity prohibited by law, or District policy or regulation.
- Employees shall not interfere with other employee's use or ability to send or receive email, nor shall they read, delete, copy, modify or forge other users' emails. Administrative assistants or secretaries may process emails for their supervisor/administrator if the supervisor/administrator requests such duties in writing. Any emails sent should be phrased with "sent by on behalf of (administrator)." Employees shall not use the District's system for the purpose of urging the support or defeat of any ballot measure or candidate including, but not limited to, any candidate for election to the governing board of the district.
- Employees shall not send email that either masks the employee's identity or indicates that the email was sent by someone else
- Employees may not disclose student information for any reason other than legitimate educational purposes, except as otherwise provided by law.

Electronic communication on District computers could reflect upon the District since all messages sent from the District include the name of the District in the electronic address.

Emailing to Distribution Groups:

The use of email distribution groups should be limited to those groups that are in direct alignment with a staff member's physical placement or job classification(s). Messages sent to groups outside of these criteria must have prior written approval by the staff member's site or department administrator (principal or director) or Technology Services Director. Written approval can consist of either a physical document or email message.

In addition to sending out approved messages directly, the administrators of each site\district department and their administrative support personnel have the ability to send email messages to groups outside of their own sites.

Fundraising Emails:

{SR050643.DOC}

AR 4040.1(f)

In order to facilitate the sharing of information regarding school or district events, fundraisers, and celebrations honoring various staff members, the "District Events" public folder is available for all employees' use.

Postings will be left in the folder for a minimum of 2 months, but can be deleted by the message creator before then. By placing Event Announcements in the "District Events" public folder, the email load on everyone's account will be reduced while still getting the information out to everyone.

Fundraising or announcement emails related to District business or school site business should not be sent to district email groups beyond a staff member's specific site without that Site's Administration and Technology Services' approval. Even announcements sent within a particular site should be stopped if the administration requests such.

Current district-wide fundraising events such as the annual Golf Tournament, United Way or Daffodil days are authorized for district wide emails.

Use of the Email System by Collective Bargaining Units or Meet and Confer Groups:

The email system may be utilized under the same guidelines provided to these groups that are consistent with the physical mail delivery system.

Policy
 Adopted: December 13, 2007
 Revised: April 30, 2008
 Revised: August 14, 2010

ELK GROVE UNIFIED SCHOOL DISTRICT
Elk Grove, California

{SR050643.DOC}

AR 6162.7(a)**Instruction****USE OF TECHNOLOGY IN INSTRUCTION****Copyrights**

Users shall strictly observe copyright laws. All employees shall ensure that software is used and duplicated in accordance with software licensing agreements. Public domain software may be duplicated and exchanged with other schools or staff. No illegal copies of copyrighted software shall be accepted or used in the district.

(cf. 6162.6 - Use of Copyrighted Materials)

Selection of Educational Software

Before ordering software, the Technology Services *Computer Equipment and Software Standards List/Price List* should be consulted - <http://intranet.egusd.net/pricelist/> - to see if the software is pre-authorized. For educational software that is not on the list, staff should visit the California Learning Resource Network website - <http://clrn.org> – to see if the software has been reviewed and approved. All electronic resources approved by CLRN are reviewed using the California State Board of Education’s three-fold criteria:

- Legal Compliance Review
- Curriculum Frameworks and Standards Alignment Match Verification
- CLRN Minimum Requirements Review*

* CLRN Minimum Requirements:

1. The resource addresses standards as evidenced in the standards match and provides for a systematic approach to the teaching of the standard(s), and contains no material contrary to any of the other California student content standards.
2. Instructional activities (sequences) are linked to the stated objectives for this ELR (electronic learning resource).
3. Reading and/or vocabulary levels are commensurate with the skill levels of intended learners.
4. The ELR exhibits correct spelling, punctuation, and grammar, unless a primary source document.
5. Content is current, accurate and scholarly, including that taken from other subject areas.
6. The presentation of instructional content must be enhanced and clarified by the use of technology through approaches which may include: access to real-world situations (graphics, video, audio); multi-sensory representations (auditory, graphic, text);

independent opportunities for skill mastery; collaborative activities and communication; access to concepts through hypertext, interactivity, or customization features; use of the tools of scholarship (research, experimentation, problem solving); simulated laboratory situations.

7. The resource is user friendly as evidenced by the use of features such as: effective help functions; clear instructions; consistent interface; intuitive navigational links.
8. Documentation and instruction on how to install and operate the ELR are provided and are clear and easy to use.
9. The model lesson/unit plan demonstrates effective use of the ELR in an instructional setting.

To order software *not* listed on the Technology Services *Computer Equipment and Software Standards List/Price List*, staff must complete the EGUSD *Software Request Form* and email, fax or mail it, along with any maintenance support documentation (if applicable) to Technology Services. For software listed on the CLRN website, simply note that on the form. The software will then be added to the standards list/price list.

Additional selection criteria for all software:

1. If the software is not in use in the district or is a new version of software that is in use in the district, the software will need to be tested by Technology Services on the EGUSD network prior to purchase to make sure it will work within the standards and constraints of the environment. Please allow 2-3 weeks for the testing process.

AR 6162.7(b)**Instruction****USE OF TECHNOLOGY IN INSTRUCTION cont'd****INTERNET Use**

The following terms and conditions shall be adhered to when staff and students use the district network and/or the INTERNET on district computers or via the district network:

The term INTERNET as used in this document refers to the public Internet, including, but not limited to, the World Wide Web, web pages, web logs (blogs), instant messaging, discussion boards, chat rooms, and other online learning communities and/or portals.

The term Web Page is defined as an actual HTML page, blog page, portal entry, or other representation/depiction on the Internet.

The term district network as used in this document refers to any connection made to the district network either via physical connection or wireless connection. The term password as used in this document refers to any password or password device that may be used to generate a onetime password, used to access the network or any network device or application.

1. Users who want to access the INTERNET must complete the [Application for Educational Use of the INTERNET](#). Students must complete the form annually.

2. The district makes no guarantees of any kind, whether expressed or implied, for the service it is providing. The district will not be responsible for any damages suffered by a user and makes no guarantee of access to sites. This includes loss of data resulting from delays, nondeliveries, misdeliveries, or service interruptions caused by its own negligence or user errors or omissions. Use of any information obtained via the INTERNET is at the user's risk.

3. Users of the district network and/or INTERNET have a responsibility to assist in maintaining the security of the network. Therefore, users shall adhere to the following security regulations:

- Users shall only use accounts assigned to them.
- Users shall not attempt to log-in to accounts or systems for which they do not have authorized access.
- Users must protect their password. Users should change their password periodically.
- Users shall not use non-district computers, network devices or printers on the network without written authorization from Technology Services.
- Users shall maintain their password(s) as confidential. Users shall not give their password to anyone. This includes, but is not limited to, students, TA's, Technology Services, colleagues, and administrators.
- Users shall memorize their password.
- Users shall not write their password on a sticky note or piece of paper where it can be found. This includes: Hiding it under their keyboard or placing it on their monitor or in their desk drawer.

- Users shall lock the workstation or log out before leaving.
- Users shall not leave their computer unlocked when they are out of the room.
- Users shall log out if someone else needs to use the computer – they will have them login using their own username and password.
- Users shall not leave their workstation unattended while they are logged on.
- Users shall use the password feature of their screen saver.
- Users shall not allow anyone to use their email account to send email.
- Users shall not allow anyone to use their system accounts to work. If a person does not have the proper capabilities to do a task, he/she should contact Technology Services so the appropriate capabilities can be provided.
- Users shall not plug in wireless access points unless approved and authorized by Technology Services.
- Users shall not download confidential student or employee information onto laptops, desktops or other portable storage devices without authorization from the Director of Technology Services or designee. Authorized loading of confidential information onto laptops or other portable storage devices should only be done utilizing secure encryption.

• 5. Acceptable Use - The INTERNET including, but not limited to, the World Wide Web, blogs, discussion boards, chat rooms, and other online learning communities and/or portals is intended to be used in support of, and be consistent with, the educational standards and benchmarks of the district. Users will be provided access to the INTERNET in accordance with the District INTERNET filtering and blocking measures. These measures are in place to avoid access to inappropriate material that is not consistent with the educational standards and benchmarks of the district. Student access to INTERNET services is provided under staff supervision. Additionally, students will receive age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such instruction shall include, but not be limited to, the dangers of posting personal information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying.

6. Unacceptable Use - The transmission or reception of any material in violation of any applicable laws, regulations, or district policies is prohibited. This includes but is not limited to, the misuse of copyrighted material or material protected by trade secret. Any transmission or reception of material by a student that is obscene, libelous, slanderous, gang-related, or incites students and/or staff so as to create a clear and present danger of: a) the commission of unlawful acts on school premises, b) the violation of lawful school regulations, or c) the substantial disruption of the orderly operation of the school, is prohibited and shall result in the termination of a user's INTERNET privileges and/or appropriate disciplinary actions. Prohibited "gang-related" materials are further described in BP/AR 5131.

7. Privileges - The use of information technology is a privilege, and unacceptable use by students, as described in number six above, shall result in the cancellation of those privileges

and/or appropriate disciplinary actions. The system administrator may close an account at any time as required. The principal/designee of any school may request the system administrator deny, revoke, or suspend a user's account.

8) Network Etiquette - Users are expected to abide by the generally accepted guidelines of network etiquette. These include (but are not limited to) the following:

- Users shall be polite, respectful and brief. Sarcasm, humor and using all caps may be misinterpreted as being rude.
- Users under age 18 shall not reveal their last names, addresses or phone numbers.
- Electronic mail (e-mail) is not guaranteed to be private and users acknowledge that they have no expectation of privacy. E-mail messages related to or in support of illegal activities shall be reported to an administrator who shall notify Technology Services and Police Services. Messages sent via e-mail using the District's network or server(s) are a limited forum, similar to the school newspaper, and therefore, the District, the principal, or the classroom teacher may restrict student speech for valid educational reasons as set forth within Education Code section 48907. The District will not restrict a student's speech on the basis of a disagreement with the opinions a student expresses. Employees' use of email is governed by BP 4040.1 (a) EMPLOYEE USE OF EMAIL.
- Network use that disrupts the use of the network by others is unacceptable.
- Users are required to obey the copyright laws and all other applicable laws and regulations.

9. If a student commits vandalism which constitutes a violation of Education Code section 48900 (f), the student may be subject to disciplinary action for such vandalism in accordance with existing policies and the Education Code. Vandalism shall result in the cancellation of privileges under this policy. Vandalism is defined as the willful or malicious destruction of public property. Vandalism includes, but is not limited to, the creation or uploading of computer viruses and/or harming or destroying data of another user or network, or a compromise (a breach, hacking, unauthorized access, suspected unauthorized changes, deletions, additions, or viewing) to one or more of the District's Enterprise Data Systems (SISWeb, QSS, Email, Network Accounts; any system used district or school wide). Students may also be subject to disciplinary action under other relevant grounds for violation of this policy and other applicable policies.

10. Theft or Damage to Electronic Files or Data Bases (Computer System Tampering or Hacking)

In the event that the system has been compromised or believed to have been compromised the following guidelines have been established.

Any employee, upon learning that a compromise (a breach, unauthorized access, suspected unauthorized changes, deletions, additions, or viewing) to one or more of the District's Enterprise Data Systems (SISWeb, QSS, Email, Network Accounts; Any system used district or school wide) has potentially occurred, shall notify immediately, their supervisor who shall notify the appropriate Associate Superintendent and the Director of Technology Services to initiate a prompt investigation.

The appropriate District Administrator, Director of Elementary, Secondary Education, or Adult Education shall notify the following departments of the potential compromise and investigation:

- Superintendent (Who will inform the Board of Education or designate a person who will inform the Board of Education of the investigation)
- Principal or Department Manager
- Police Services
- Technology Services
- Communications
- Student Services (student involvement suspected/confirmed)
- Human Resources (staff involvement suspected/confirmed)
- Risk Management

School or department administration will contact the Director of Technology Services and the Chief of Police as the first step when initiating an investigation. Alleged offenders should not be interviewed or notified of suspicions at this stage unless agreed to by the Director of Technology Services and the Chief of Police. In collaboration with Police Services and Technology Services, the school or department will utilize all available resources including but not limited to Human Resources and the Office of Student Services and appropriate Law Enforcement agencies as deemed necessary.

Prior to issuing any discipline or recommending disciplinary action to any alleged student offenders a review of findings will be provided to Human Resources and/or the Office of Student Services. Coordination as appropriate with Law Enforcement shall include, but not be limited to Sacramento County Sheriff's Department, High Tech Crime Unit, with guidance from Sacramento County District Attorney's staff, who will conduct their own investigation as appropriate. The District will provide them with complete access to all information the school or Technology Services may have obtained subject to any confidentiality requirements related to student or employee records.

School or department administration, working with Technology Services will keep time and cost accounting logs documenting the staff hours for the investigation for possible restitution and evidence for any disciplinary hearing. The investigation will be treated as a high priority by Technology Services and Police Services, recognizing that time is of the essence.

School or department administration will coordinate an incident review meeting that involves Police Services, Technology Services, identified department management and the appropriate Associate Superintendent. Upon reviewing the results of the investigation, a decision about disciplinary action for the alleged student offenders will be recommended to the Superintendent.

School or department administration in consultation with the Office of Student Services will conference with alleged offender(s) in order to inform them of the reason for disciplinary action and allow an opportunity to present their version and evidence in defense of the alleged violations prior to the school issuing a suspension and notifying the parent or guardian of the disciplinary action.

Employees who violate this policy may be disciplined in accordance with the provision of District policies and the provision of appropriate employee collective bargaining

agreements. When the alleged offender is an employee of the District, she/he must be made aware of, and afforded their right to representation.

All media requests shall be coordinated through the Communications Department. School Administration shall immediately advise the Communications Department if the media arrives at the school campus.

Web Page Design

Access to the INTERNET through the Elk Grove Unified School District and creation of a Web Page using the District's network or server and as part of the educational program is a limited forum, similar to the school newspaper, and the District will exercise its rights within the law to regulate speech within that forum. Therefore, the district, the principal, or the classroom teacher may restrict student speech pursuant to Education Code section 48907 if the speech is obscene, libelous, slanderous, or likely to incite students and create a clear and present danger to the operation of the schools, or otherwise interferes with the educational mission of the district. The district will not restrict a student's speech on the basis of a disagreement with the opinions a student expresses. Web Pages are defined as actual HTML pages, blog pages, portal entries or other representation/depiction on the World Wide Web.

The following shall be adhered to when staff design Web Pages for display, or utilize web pages on the INTERNET in connection with their work, or post or allow the posting, of student web pages or student work:

All web pages must conform to the applicable sections of BP 1113:

All website content on district and school websites/pages shall protect the privacy rights of students, parents/guardians, staff, Board members, and other individuals.

(cf. 1340 - Access to District Records)

(cf. 4119.23/4219.23/4319.23 - Unauthorized Release of Confidential/Privileged Information)

(cf. 5022 - Student and Family Privacy Rights)

(cf. 5125 - Student Records)

Phone numbers, home addresses, and email addresses of students or their parents/guardians shall not be published on an external district or school webpage unless parent/guardian written permission is obtained. Only district approved administrative systems which are closed systems requiring a logon and password may contain all student information.

(cf. 5125.1 - Release of Directory Information)

First and last names of students *without* images or identifiable images of students *without* first or last names may be published except when the student's parent/guardian has notified the district in writing, using the appropriate opt-out form, which forbids the release of the student's information.

The publication of student image(s) along *with* both first and last name requires prior written consent of the student's parent/guardian.

Home addresses or personal telephone numbers of staff members shall not be posted on district and school websites/pages.

No public safety official shall be required as a condition of employment to consent to the posting on the Internet of his/her photograph or identity as a public safety officer for any purpose if that officer reasonably believes that the disclosure may result in a threat, harassment, intimidation, or harm to the officer or his/her family. (Government Code 3307.5)

DISTRICT AND SCHOOL WEBSITES

District and school websites/pages shall not post the home address or personal telephone number of any elected or appointed official including, but not limited to, a Board member or public safety official, without the prior written permission of that individual. (Government Code 3307.5, 6254.21, 6254.24)

(cf. 3515.3 - District Police/Security Department)

1. Web pages must support course objectives and be educationally informative.
- 2.
3. Parent/guardian written permission must be obtained and teacher/administrator approval before a video is posted containing students and before a video conferencing session involving students begins.
4. Electronic Student Newspapers are required to follow these same requirements.
- 6.

The following shall be adhered to regarding Student Web Pages:

1. Students will receive instruction on the design of Web Pages.
2. A teacher or administrator may authorize the posting of Student Web Pages (and/or student work) that support course objectives or are educationally informative on an Elk Grove Unified School District web page if student and parent/guardian written permission is obtained before posting. Additionally, any student work that contains photos or videos of other students must comply with requirements of this regulation prior to posting.

Policy
 Adopted: July 5, 1994
 Revised: April 6, 1998
 June 17, 2002

ELK GROVE UNIFIED SCHOOL DISTRICT
Elk Grove, California

December 7, 2005
 January 4, 2006
 April 30, 2008
 September 16, 2010
 September 21, 2011

AR 6162.7(f)

Instruction

USE OF TECHNOLOGY IN INSTRUCTION

Application for Educational Use of the INTERNET

I have read, understand and will abide by the attached Terms and Conditions, Board Policy and Administrative Regulation, for INTERNET access. I further understand that any violation of the Terms and Conditions is improper and may constitute an administrative, civil or criminal offense. Any violation may result in my access privileges being revoked. Additional disciplinary action and/or appropriate legal action may be taken. I further understand that electronic mail (e-mail) is not guaranteed to be private and acknowledge that I have no expectation of privacy. E-mail messages related to or in support of illegal activities shall be reported to the authorities.

My signature indicates that I understand that the District Board makes no guarantees of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages I suffer. This includes loss of data resulting from delays, nondeliveries, misdeliveries, or service interruptions caused by its own negligence or my errors or omissions. Use of any information obtained via the INTERNET is at my own risk.

My Name: _____ Date: ____/____/____
 (Please print Name)

Home Address: _____
 Street City State Zip

X _____
 Signature Student ID# Grade Level

X _____
 Parent/Guardian's signature if the user is less than 18 years of age

The signatures indicate that the user has read and agrees to the attached Board Policy and Administrative Regulation for INTERNET Access.

EMPLOYEE ACCEPTABLE USE AGREEMENT FOR INTERNET AND OTHER ELECTRONIC RESOURCES

Electronic Resources

The Elk Grove Unified School District ("District") recognizes the value of District computers and other electronic resources, as well as personal electronic devices, to improve student learning and enhance the administration and operation of its schools. To this end, the District encourages the responsible use of computers; computer networks, including the Internet and Internet2; and other electronic resources in support of the mission and goals of the District and its schools. Users are reminded that the District e-mail system and all user accounts are owned by the District, and all electronic mail activity which utilizes the District server is monitored and logged. Every attempt is made to scan all electronic mail coming into or leaving the organization for viruses and for offensive material. Additionally every effort is made to log and monitor all web traffic for inappropriate or offensive content.

As used in this Agreement, "personal electronic devices" may include but are not limited to, cellular telephones, personal digital assistants ("PDAs"), and portable laptop computers, or any other device with wireless capabilities provided to the employee by the district.

Acceptable Use and General Rules of Usage

Use of District computers and other electronic resources or use of the wireless capability features of any personal electronic device is intended to be used in support of, and be consistent with, the educational standards and benchmarks of the District. Users will be provided access to the INTERNET in accordance with the District INTERNET filtering and blocking measures. The measures discussed below are in place to avoid access to inappropriate material that is not consistent with the educational standards or professional norms and benchmarks of the District.

Acceptable Use

1. Exhibit exemplary behavior on the network or while using District electronic equipment and while using the wireless capability features of any personal electronic device.
2. Network accounts are to be used only by the authorized user of the account for authorized purposes.
3. For District employees provided with email, the email is considered a primary avenue of communication and should be checked by employees frequently.
4. Communications and information accessible via the network are subject to monitoring and/or review at any time and should not be assumed to be private.
5. Any employee, upon learning that a compromise (a breach, unauthorized access, suspected unauthorized changes, deletions, additions, or viewing) to one or more of the District's Enterprise Data Systems (SISWeb, QSS, Email, Network Accounts; any system used District or school wide) has potentially occurred, shall immediately notify his or her supervisor who shall notify the appropriate Associate Superintendent and the Director of Technology Services to initiate a prompt investigation.
6. As necessary, the District will make determinations on whether specific uses of the network or personal electronic devices are consistent with the acceptable use practice.

Unacceptable Use

1. Giving out personal or confidential information about another employee or student, including home address and phone number without appropriate authorization, is strictly prohibited.
2. Any use of the District systems or technology resources for commercial or political purposes is prohibited.
3. Excessive use of the District systems or technology resources for personal business is prohibited.
4. Any use of the District systems or technology resources for political lobbying is prohibited.
5. Users shall not use non-District computers or printers on the network without written authorization from Technology Services.
6. Users shall only use accounts assigned to them and shall not attempt to log-in to accounts or systems for which they do not have authorized access.
7. Users shall not allow others to use their accounts.
8. Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the network. District policies for the use and protection of passwords can be found in AR 6162.7.

9. No use of the District's systems or technology resources shall serve to disrupt the use of the network by others. Hardware and/or software shall not be destroyed or abused in any way. Modifications to system configurations should not be made without written authorization from Technology Services.
10. Users shall not plug in wireless access points unless approved and authorized by Technology Services.
11. Malicious use of the District's systems or technology resources to develop or use programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited.
12. Hate mail, chain letters, harassment, discriminatory remarks, cyber-bullying and other antisocial behaviors are prohibited on the network. In accordance with BP 0201, Human Dignity Policy, the school district will not tolerate behavior by students, staff, or visitors which insults, degrades, or stereotypes any race, gender, disability, physical characteristics, ethnic group, sexual orientation, age, national origin, or religion.
13. The unauthorized installation of any software, including shareware and freeware, for use on Elk Grove Unified School District computers is prohibited. Contact Technology Services in advance for authorization.
14. Users shall not disclose student information for any purpose other than a legitimate educational purpose, or as otherwise permitted by law.
15. Use of the network or personal electronic devices to intentionally access or process pornographic or adult sites with explicit sexual content or other inappropriate or derogatory material, inappropriate texting or messaging, or files dangerous to the integrity of the local area network is prohibited.
16. The Elk Grove Unified School District network may not be used for downloading entertainment software, music, videos or other files not related to the mission and objectives of the Elk Grove Unified School District. This prohibition pertains to freeware, shareware, copyrighted commercial and non-commercial software, and all other forms of software and files not directly related to the instructional and administrative purposes of the Elk Grove Unified School District.
17. Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner is prohibited, except when duplication and/or distribution of materials for educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law.
18. Use of the District's systems, network or technology resources for any unlawful purpose is prohibited.
19. Users shall not download confidential student or employee information onto laptops, desktops or other portable storage devices without authorization. Authorized loading of confidential information onto laptops or other portable storage devices should only be done utilizing secure encryption.

A breach of this Agreement may lead to revocation of access privileges, disciplinary action, up to and including dismissal, and/or appropriate legal action.

I have read, understand, and will abide by the above agreement, all applicable District Board Policies and Regulations, Technology Services Department Official Procedures and Protocols, and applicable state and federal laws, when using computer and other electronic resources owned, leased, or operated by the Elk Grove Unified School District. I understand that this agreement will be in effect during the entire time of my employment with the District. Any subsequent changes to the agreement will be posted online and will be communicated electronically to employees and will be sent to employees for signature.

Employee Name (Full Name)	
Employee ID	



Signature: _____

Date: _____

Revised 12/16/08

ALL EMPLOYEES MUST REVIEW, SIGN, AND RETURN THIS FORM TO TECHNOLOGY SERVICES

Instruction**USE OF TECHNOLOGY IN INSTRUCTION**

The Elk Grove Unified School District (District) Board of Education (Board) encourages the instructional use of computers, videotapes, interactive videodisks, distance learning, cable television and other technologies. The Board perceives that these technologies:

- a) give students new ways to access information and practice skills;
- b) help teachers meet a wide range of learning styles;
- c) enable teachers to move from whole-class instruction to a mixture of small-group and individualized instruction;
- d) help students develop reasoning and problem-solving abilities and,
- e) will be a part of each student's everyday life.

The Board recognizes that trained staff are needed to make the best use of the district's technology. Staff shall receive training in using the technologies available to them. All district schools shall have the opportunity to obtain computers, software and other equipment.

The district's educational software shall be carefully selected and evaluated so as to meet the staffs' and students' needs and conform with district policy and regulations. Software requests will be compared to published lists of recommended titles to assure educational appropriateness. Multiple copy purchases of a software title will follow the same procedure as the district's textbook adoption process.

INTERNET access shall be available for staff and students. The use of the INTERNET shall be evaluated so as to meet the staffs' and students' needs and conform with District policy and regulations. Before using on-line services, the staff or student and parent/guardian shall sign the District's *Application for Educational Use of the INTERNET* indicating that the user will abide by the conditions and understands that the District makes no guarantee to provide access to all INTERNET sites and has no rights to privacy.

The Superintendent or designee shall establish administrative regulations governing the use of the district's on-line services. She/He shall ensure that the users have no expectations of privacy and understand that the district staff may monitor or examine all on-line activities to ensure proper use of the system. Users who fail to abide by these regulations shall be subject to disciplinary action, revocation of user privileges, and legal action as appropriate.

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that prevents access to visual depictions that are obscene, child pornography, or – with respect to use of computers with Internet access by minors – harmful to minors and that the operation of such measures is enforced. The Superintendent or designee may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose.

The Superintendent or designee shall ensure that;

BP 6162.7 (b)**Instruction****USE OF TECHNOLOGY IN INSTRUCTION**

- Access by minors to inappropriate matter on the Internet and World Wide Web is restricted via a technology protection measure.
- The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications is secured via a technology protection measure to the extent possible.
- Administrative regulations prohibiting unauthorized access including “hacking” and other unlawful activities by minors or staff are established.
- Administrative regulations prohibiting the unauthorized disclosure, use, and dissemination of personal information regarding minors are established.
- Measures designed to restrict minors’ access to materials harmful to minors are established.
- Age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services is provided. Such instruction shall include, but not be limited to, the dangers of posting personal information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying.

The principal or designee shall ensure that all students using technology resources receive training in their proper use as well as copies of the district’s acceptable use policy and regulations.

(cf. 3512 - Equipment)
 (cf. 4132 - Publication or Creation of Materials)
 (cf. 6161.1 - Selection and Evaluation of Instructional Materials)
 (cf. 6161.11 - Supplementary Instructional Materials)
 (cf. 6162.6 - Use of Copyrighted Materials)

Legal Reference:

EDUCATION CODE
 51865 California distance learning policy
 51870-51884 Educational Technology Act of 1992
 GOVERNMENT CODE
 3543.1 Rights of employee organizations
 PENAL CODE
 502 Computer crimes, remedies
 632 Eavesdropping on or recording confidential communications
 UNITED STATES CODE, TITLE 20
 6801-6979 Technology for Education Act
 7001 Internet safety policy and technology protection measures, Title III funds
 UNITED STATES CODE, TITLE 47

BP 6162.7 (c)

Instruction**USE OF TECHNOLOGY IN INSTRUCTION**

254 Universal service discounts (E-rate)

CODE OF FEDERAL REGULATIONS, TITLE 47

54.520 Internet safety policy and technology protection measures, E-rate discounts

ELK GROVE UNIFIED SCHOOL DISTRICT
Elk Grove, California

Policy

Adopted: July 5, 1994

Revised: April 6, 1998

June 17, 2002

November xx, 2011