Issue | Background | Findings | Conclusions | Recommendations | Responses | Attachments

Summary of Keeping High School Student Records Private

Issue

Do high schools in San Mateo County have sufficient guidelines and policies to safeguard electronic portable storage of sensitive student data consistent with California law?

Summary

The San Mateo County Civil Grand Jury (Grand Jury) asked high school district officials in the County if they had policies, in addition to the California Education Code statutory requirements, that specifically address faculty and administrator laptop computer usage and other off-site storage of student records. The Grand Jury found that none of the high school districts in the county had such specific policies or guidelines regarding these matters.

The Grand Jury recommends that the school districts develop by February 1, 2007, policies and guidelines specific to their own situation for the off-site storage of personal student information similar to those policies and guidelines issued by the San Mateo County Office of Education. Also, the Grand Jury recommends that the school districts train faculty and administrators in the proper off-site storage of personal student information, and obtain signed employee statements acknowledging that they have read and will comply with the policies.

Keeping High School Student Records Private

Issue

Do high schools in San Mateo County have sufficient guidelines and policies to safeguard electronic portable storage of sensitive student data consistent with California law?

Background

The theft of laptop computers and the accompanying compromise of personal information have received recent media attention. The California Education Code makes reference to student record security but does not provide specific guidelines for laptop computers and other off-site storage media such as USB flash memory sticks. While off-site access to administrative systems better enables approved employees to process work and meet deadlines, it is important that school districts keep student information private pursuant to California Education Code § 49060 et seq. and the Federal Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99).

Traditionally, teachers work on student assignments and examinations at home. This provides the faculty with some flexibility in the grading process. Computers provide an efficient tool to manipulate and store data, and faculty use laptop computers off-site to assist in their grading.

Student grades are considered "personal information." The loss of this information through, for instance, theft of a laptop computer or the loss of a USB flash memory stick containing student names, grades or any other personal information, could violate personal information privacy laws.

The San Mateo County Office of Education (SMCOE) has prepared guidelines (see Appendix A) for SMCOE employees to access administrative records off-site. These guidelines help employees satisfy the California personal privacy statutes and specifically address what is considered acceptable treatment of personal student information residing on laptop computers and off-site storage media. The guidelines include:

1. An annual inspection of all SMCOE laptops by Information Technology Services personnel,

2. A ban on unauthorized person's use of SMCOE laptop computers,

3. A ban on printing student or family information off-site,

4. A requirement that off-site users encrypt or password-protect all personal student information.

Additionally, SMCOE requires that all faculty and administrators understand and abide by these requirements by annually requiring a signature acknowledging these policies.

Investigation

The San Mateo County Civil Grand Jury (Grand Jury) limited its investigation to the seven school districts in San Mateo County that have high schools. The Grand Jury asked the superintendent in each of these districts to provide a copy of that district's policies, in addition to the Education Code guidelines, that address faculty and administrator laptop computer storage of student records.

Findings

None of the high school districts in San Mateo County had guidelines other than the California Education Code for the secure off-site storage of personal student information.

Conclusions

Districts with high schools in San Mateo County should prepare and implement guidelines to secure personal student information residing on laptop computers and off-site storage media.

Recommendations

The Grand Jury recommends that the Boards of Trustees of Cabrillo Unified School District, Jefferson Union High School District, LaHonda-Pescadero Unified School District, Ravenswood City School District, San Mateo Union High School District, Sequoia Union High School District and the South San Francisco Unified School District:

1. Develop policies and guidelines specific to their own situation for the off-site storage of personal student information similar to the policies and guidelines issued by the San Mateo County Office of Education. These policies and guidelines should be implemented by February 1, 2007.

2. Should make their employees aware of the importance of these policies by:

   2.1. Training faculty and administrators on the proper off-site storage of personal student information, and

   2.2. Obtaining signed employee statements acknowledging that they have read and will comply with these policies and procedures.

Appendix A

EMPLOYEE OFF-SITE PERSONAL DATA HANDLING POLICY

(revised 08/17/06)

The San Mateo County Office of Education (SMCOE) permits off-site access to administrative systems and/or off-site access to paper or electronic documents containing personal data to approved employees. The purpose of this access is to better enable approved employees to process work and meet deadlines. It is the responsibility of SMCOE employees accessing administrative applications from off-site locations to maintain the security of this information by following all SMCOE policies and procedures and abiding by all applicable personal information privacy laws as stated below. It is equally important for SMCOE employees transporting equipment and/or documents containing personal data to maintain the security of this information at all times. Failure to abide by these policies, procedures and laws may result in the loss of access to SMCOE systems and/or legal consequences.

For the purposes of this document, SMCOE administrative systems will include, but not be limited to, any student system, special education system, business system, or personnel / HR system that contains personal information related to individual students, employees, or their family members.

APPLICABLE LAWS

California Penal Code § 502 – Unauthorized access to computers, computer systems and computer data: This section provides that any person who commits one of the acts listed below is guilty of a public offense. SMCOE considers any use of SMCOE computer systems or access to any SMCOE-owned data containing personal information with the intent to commit one of the listed offenses to be "without permission." Listed offenses include but are not limited to:

1) damaging, deleting, destroying or using any data to defraud, deceive, extort or wrongfully control or obtain money, property or data
2) using computer services without permission
3) assisting unauthorized persons in the use of computer services without permission
4) assisting unauthorized persons in gaining access to documents containing personal data without permission
5) altering, deleting, adding or destroying hardcopy documents or electronic data on SMCOE systems without permission
6) disrupting computer services or causing the denial of computer services to an authorized user
7) knowingly introducing any computer contaminant into any computer, computer system or computer network.

SMCOE is obligated to report all violations of the above section to the appropriate authorities, which may lead to fines of up to $10,000 and/or imprisonment of up to three years.

For the purposes of this document, the term "personal information" is defined as stated in **California Civil Code Section 1798.80-1798.84:**

1) "Personal information" means an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
    a. social security number
    b. driver's license number or California identification card number
    c. account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
    d. medical information
2) "Medical information" means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional.
3) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

The full text of **California Civil Code Section 1798.80-1798.84** can be found at:
http://www.aroundthecapitol.com/code/code.html?sec=civ&codesection=1798.80 -1798.84

TERMS AND CONDITIONS

Off-site access to any SMCOE administrative system is subject to the following:

1) Employees requesting off-site access to SMCOE's administrative systems and/or permission to transport SMCOE data containing personal information must sign and adhere to the rules and policy as stated in this document.

2) Off-site access to SMCOE administrative systems requires the written authorization of both the employee's immediate supervisor and the division head. A copy of the written authorization is to be kept on file by Information Technology Services (ITS) for a period of two years.

3) Off-site access to SMCOE administrative systems is limited to secured channels as established and configured by ITS.

4) Off-site access to SMCOE administrative systems is limited to SMCOE laptops. The laptops are to be automatically scanned for viruses, Trojans, spyware and other malware upon connection to any SMCOE network.

5) SMCOE laptops must be inspected annually by ITS personnel for the presence of malware, applications not owned by SMCOE, or any other program that could compromise the integrity of the SMCOE network or SMCOE administrative systems.

6) Off-site users of SMCOE laptops must not allow any non-authorized person to access the machine for any reason at any time. Passwords cannot be shared with non-authorized persons at any time.

7) SMCOE laptops connecting to SMCOE administrative systems must be user-defined and authenticated upon entry into the SMCOE network. All applications must be password protected. All administrative applications must time out after 30 minutes of inactivity and can only be re-accessed with a password. No personally owned software is to be installed on SMCOE laptops.

8) Off-site users of SMCOE administrative systems are not to print off-site any screen captures, reports or other hard-copy documents that contain personal or confidential information regarding any SMCOE student, staff member, or a family member of any SMCOE student or staff member.

9) Off-site users of SMCOE administrative systems shall not save on any drive of their laptop or any portable machine (including portable media) data that contain personal or confidential information regarding any SMCOE student, staff member, or a family member of any SMCOE student or staff member unless the data are encrypted or password protected.

10) Any personal data as defined by California Civil Code Section 1798.80-1798.84 that is transported electronically or physically shall not be saved on the hard drive of any personally owned machine or any non-SMCOE machine, even if the data are to be stored temporarily. Employees needing to work electronically with personal data as defined by California Civil Code Section 1798.80-1798.84 must save the data to SMCOE-purchased portable media that encrypts or password protects the data and work exclusively from that media.

11) Employees must return SMCOE equipment (including portable media) when on a leave of absence. Upon separation of employment, employees must immediately return all SMCOE equipment. SMCOE retains the right to withhold the employee's final paycheck until all SMCOE equipment has been returned.

12) All users must report a systems security breach to the ITS administrator or designee immediately upon discovery.

SMCOE POLICY

1) SMCOE maintains the right to monitor all activity involving the use of SMCOE's administrative systems at any time without prior notice.

2) SMCOE retains the right to terminate access to any SMCOE system at any time without prior notice.

3) All data collected, printed and/or stored on any device owned or leased by SMCOE is the property of SMCOE.

4) SMCOE retains the right to amend its policy and/or rules at any time without prior notice.

5) Employees understand that they will be held liable for any financial damages resulting from their illegal use of SMCOE's administrative systems.

ACCEPTABLE USE POLICY ACKNOWLEDGEMENT STATEMENT

I, _____, have read and understand the above Terms and Conditions of Use and agree to abide by them. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, I may be subject to disciplinary action, from termination of technology access privileges up to termination of employment. Appropriate legal action may also be taken.

Signature of User: _____ Date: _____/_____/_____

Name (print): _____ Phone Number: (____) _____

Position / Program: _____ Division: _____

Signature of Supervisor: _____ Date: _____/_____/_____

Signature of Division Head: _____ Date: _____/_____/_____

January 3, 2007

Honorable John L. Gransaert
Judge of the Superior Court
Hall of Justice
400 County Center, 2nd Floor
Redwood City, CA 94063-1655

RE: KEEPING HIGH SCHOOL STUDENT RECORDS PRIVATE Report

Dear Judge Grandsaert,

This letter is in response to your letter dated October 12, 2006 regarding KEEPING HIGH SCHOOL STUDENT RECORDS PRIVATE. The Cabrillo Unified School District understands the need for security regarding off-site storage of student personal information. The Cabrillo Unified School District does not have any off-site storage nor does it allow external utilization of student information off-site.

Therefore, the Grand Jury report finding is un-warranted regarding Cabrillo Unified School District.

The district administration feels it is important to develop a policy similar to San Mateo County Office of Education's policy. We therefore agree with the finding and will implement a similar policy by June 2007 regarding student information in case the district utilizes off-site storage in the future.

Sincerely,

John Bayless, Ed.D.
Superintendent

JB/cmd

Jefferson Union High School District

ADMINISTRATIVE OFFICES – SERRAMONTE DEL REY
699 Serramonte Boulevard, Suite 100
Daly City, CA 94015-4132
650-550-7900 • FAX 650-550-7888

October 24, 2006

The Honorable John L. Grandsaert
Judge of the Superior Court
Hall of Justice and Records
400 County Center, 2nd Floor
Redwood City, California 94063-1655

Dear Judge Grandsaert:

The Jefferson Union High School District has reviewed the recent findings and recommendations of the San Mateo County Grand Jury related to policies safeguarding sensitive student information on portable electronic storage devices.

The District finds the recommendations appropriate given the expanded role of portable electronic storage in educational communities. While the Jefferson Union High School District has limited use of these devices, the District agrees with the findings and recommendations.

The Jefferson Union High School District has initiated a process to develop operable guidelines and district policies as recommended. These policies and guidelines will be presented to the Board of Trustees for adoption following the suggested Grand Jury timeline. Training will be provided to those impacted by the policy.

Sincerely,

Michael J. Crilly
Superintendent

c Board of Trustees

LA HONDA-PESCADERO UNIFIED SCHOOL DISTRICT
P.O. Box 189 • 620 North Street, Pescadero, CA 94060
650-879-0286 • FAX 650-879-0816

Timothy A. Beard, Superintendent

A Lighthouse District

January 23, 2007

Hon. John L. Grandsaert
Judge of the Superior Court
Hall of Justice
400 County Center, 2nd floor
Redwood City, CA 94063-1655

Hon. Judge Grandsaert:

This letter is in reference to the 2006-07 County Grand Jury report on "Keeping High School Student Records Private". The La Honda-Pescadero Unified School District has considered the Grand Jury's findings and submits this letter in response to the recommendations to high school districts.

By February 1, 2007, our district will implement the attached policy on how employees should protect personal information when working off-site. This policy is modeled on the San Mateo County Office of Education's policy on "Employee Off-Site Personal Information Handling Policy." Implementation of this policy will also include the following:

- Training staff on the proper protection of personal student information
- Signed statements by staff acknowledging that they have read and will comply with this policy

The La Honda-Pescadero Unified School District agrees with the Grand Jury that the security of personal student information is of the utmost importance, and the findings of this report will be helpful to us as we implement our plan to address this issue.

Sincerely,

Timothy A. Beard,
District Superintendent

La Honda-Pescadero Unified School District
EMPLOYEE OFF-SITE PERSONAL INFORMATION HANDLING POLICY

The La Honda-Pescadero Unified School District (DISTRICT) permits off-site access to administrative systems and/or off-site access to paper or electronic documents containing personal data to approved employees. The purpose of this access is to better enable approved employees to process work and meet deadlines. It is the responsibility of DISTRICT employees accessing administrative applications from off-site locations to maintain the security of this information by following all DISTRICT policies and procedures and abiding by all applicable personal information privacy laws as stated below. It is equally important for DISTRICT employees transporting equipment and/or documents containing personal data to maintain the security of this information at all times. Failure to abide by these policies, procedures and laws may result in the loss of access to DISTRICT systems and/or legal consequences.

For the purposes of this document, DISTRICT administrative systems will include, but not be limited to, any student system, special education system, business system, or personnel / HR system that contains personal information related to individual students, employees, or their family members.

TERMS AND CONDITIONS

Off-site access to any DISTRICT administrative system is subject to the following:

1) Employees requesting off-site access to the DISTRICT's administrative systems and/or permission to transport DISTRICT data containing personal information must sign and adhere to the rules and policies as stated in this document.

2) Off-site access to DISTRICT administrative systems requires the written authorization of both the employee's immediate supervisor. A copy of the written authorization is to be kept on file by the District for a period of two years.

3) Off-site access to DISTRICT administrative systems is limited to secured channels as established and configured by the District.

4) Off-site access to DISTRICT administrative systems is limited to DISTRICT laptops. The laptops are to be automatically scanned for viruses, Trojans, spyware and other malware upon connection to any DISTRICT network.

5) DISTRICT laptops must be inspected annually by District personnel for the presence of malware, applications not owned by DISTRICT, or any other program that could compromise the integrity of the DISTRICT network or DISTRICT administrative systems.

6) Off-site users of DISTRICT laptops must not allow any non-authorized person to access the machine for any reason at any time. Passwords cannot be shared with non-authorized persons at any time.

7) DISTRICT laptops connecting to DISTRICT administrative systems must be user-defined and authenticated upon entry into the DISTRICT network. All applications must be password protected. All administrative applications must time out after 30 minutes of inactivity and can only be re-accessed with a password. No personally owned software is to be installed on DISTRICT laptops.

8) Off-site users of DISTRICT administrative systems are not to print off-site any screen captures, reports or other hard-copy documents that contain personal or confidential information regarding any DISTRICT student, staff member, or a family member of any DISTRICT student or staff member.

9) Off-site users of DISTRICT administrative systems shall not save on any drive of their laptop or any portable machine (including portable media) data that contain personal or confidential information regarding any DISTRICT student, staff member, or a family member of any DISTRICT student or staff member unless the data are encrypted or password protected.

10) Any personal information as defined by California Civil Code Section 1798.80-1798.84 that is transported electronically or physically shall not be saved on the hard drive of any personally owned machine or any non-DISTRICT machine, even if the data are to be stored temporarily. Employees needing to work electronically with personal information as defined by California Civil Code Section 1798.80-1798.84 must save the data to DISTRICT-purchased portable media that encrypts or password protects the data and work exclusively from that media.

11) Employees must return DISTRICT equipment (including portable media) when on a leave of absence. Upon separation of employment, employees must immediately return all DISTRICT equipment. DISTRICT retains the right to withhold the employee's final paycheck until all DISTRICT equipment has been returned.

12) All users must report a systems security breach to the site administrator or designee immediately upon discovery.

DISTRICT POLICY

1) DISTRICT maintains the right to monitor all activity involving the use of the DISTRICT's administrative systems at any time without prior notice.

2) DISTRICT retains the right to terminate access to any DISTRICT system at any time without prior notice.

3) All data collected, printed and/or stored on any device owned or leased by DISTRICT is the property of DISTRICT.

4) DISTRICT retains the right to amend its policy and/or rules at any time without prior notice.

5) Employees understand that they will be held liable for any financial damages resulting from their illegal use of the DISTRICT's administrative systems.

ACCEPTABLE USE POLICY ACKNOWLEDGEMENT STATEMENT

I, _____, have read and understand the above Terms and Conditions of Use and agree to abide by them. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, I may be subject to disciplinary action, from termination of technology access privileges up to termination of employment. Appropriate legal action may also be taken.

Signature of User: _____ *Date:* _____

Name (print): _____ *Position:* _____

Signature of Supervisor: _____ *Date:* _____

APPLICABLE LAWS

California Penal Code § 502 – Unauthorized access to computers, computer systems and computer data: This section provides that any person who commits one of the acts listed below is guilty of a public offense. DISTRICT considers any use of DISTRICT computer systems or access to any DISTRICT-owned data containing personal information with the intent to commit one of the listed offenses to be "without permission." Listed offenses include but are not limited to:

1) damaging, deleting, destroying or using any data to defraud, deceive, extort or wrongfully control or obtain money, property or data
2) using computer services without permission
3) assisting unauthorized persons in the use of computer services without permission
4) assisting unauthorized persons in gaining access to documents containing personal data without permission
5) altering, deleting, adding or destroying hardcopy documents or electronic data on DISTRICT systems without permission
6) disrupting computer services or causing the denial of computer services to an authorized user
7) knowingly introducing any computer contaminant into any computer, computer system or computer network.

DISTRICT is obligated to report all violations of the above section to the appropriate authorities, which may lead to fines of up to $10,000 and/or imprisonment of up to three years.

For the purposes of this document, the term "personal information" is defined as stated in California Civil Code Section 1798.80-1798.84:

1) "Personal information" means an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
    a. social security number
    b. driver's license number or California identification card number
    c. account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
    d. medical information
2) "Medical information" means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional.
3) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

The full text of California Civil Code Section 1798.80-1798.84 can be found at:
http://www.aroundthecapitol.com/code/code.html?sec=civ&codesection=1798.80 -1798.84

"OUR CHILDREN – OUR FUTURE"

Ravenswood City School District
ADMINISTRATIVE OFFICE
2120 Euclid Avenue, East Palo Alto, California 94303
(650) 329-2800 Fax (650) 323-1072

January 8, 2007

Hon. John L. Grandsaert
Judge of Superior Court
Hall of Justice
400 County Center, 2nd Floor
Redwood City, CA 94063-1655

Dear Hon. Stephen M. Hall,

This letter is in response to the 2006-2007 Grand Jury Report containing findings and recommendations pertaining to Ravenswood City School District's policies in regard to keeping high school student records private. We, the respondent, do not have high school students in our district, thus have no high school student records to keep private. The East Palo Alto Stanford High School charter is granted under the Ravenswood City School District. However, this high school is a direct funded charter, thus Stanford is responsible for all student records.

If you should have any further questions, please feel free to contact me at (650) 329-2800 ext. 163.

Sincerely,

Lisa Pruitt
Director of Student Services

San Mateo Union High School District

Samuel Johnson, Jr., Superintendent
Ethel C. Konopka, Associate Supt. Human Resources-Admin. Serv.
Elizabeth McManus, Associate Supt. Business Services

650 North Delaware Street - San Mateo, CA 94401-1795
(650) 558-2299
(650) 762-0249 FAX

January 4, 2007

Honorable John L. Grandsaert
Judge of the Superior Court
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA

The Board of Trustees of the San Mateo Union High School District agrees with the findings of the Civil Grand Jury as contained in its report of October 12, 2006. Additionally, the District believes the recommendation requires further analysis. The scope of that analysis shall include a determination as to whether or not the implementation of the terms and conditions of the sample policy provided in the Grand Jury Report would require additional personnel at further expense to the District in order to implement the policy. Further, that analysis shall be completed by the end of February 2007 with a subsequent recommendation to the Board of Trustees of the San Mateo Union High School District in March 2007.

Sincerely,

Samuel Johnson, Jr.
Superintendent and Secretary to the Board

SOUTH SAN FRANCISCO UNIFIED SCHOOL DISTRICT
398 B Street, South San Francisco, CA 94080-4423
(650) 877-8700 Fax: (650) 583-4717 www.ssfusd.k12.ca.us

SUPERINTENDENT
Barbara Olds

BOARD OF TRUSTEES
Emanuele N. Damonte
Shirlee Hoch
Raymond Latham
Liza Normandy
Philip J. Weise

January 8, 2007

The Honorable John L. Grandsaert
Judge of the Superior Court
Hall of Justice
400 County Center, 2nd Floor
Redwood City, CA 94063-1655

Dear Judge Grandsaert

RE: Grand Jury Recommendations, Student Information

This letter is in response to the San Mateo County Grand Jury's findings and recommendations relating to school districts' off-site storage of personal student information. The South San Francisco Unified School District's Education Technology Committee has reviewed the policy and regulation adopted by the San Mateo County Office of Education. The District shall present a similar policy and regulation to the District's Board of Trustees and shall recommend that the Board adopt same on or about February 8, 2007.

If you have any questions, or if you require any additional information, please do not hesitate to contact me directly.

Sincerely

Barbara Olds

Barbara Olds
Superintendent

/cc
cc: Board of Trustees
John C. Fitton, Court Executive Officer
Thomas F. Casey III

Sequoia Union High School District

480 JAMES AVENUE, REDWOOD CITY, CALIFORNIA 94062-1098

Administrative Offices (650) 369-1412

August 23, 2007

Refer to: PRG 1404

Hon. John L. Grandsaert
Judge of the Superior Court
County of San Mateo
Hall of Justice
400 County Center, 2nd Floor
Redwood City, CA 94063-1655

Re: 2006-07 Grand Jury

Dear Judge Grandsaert:

The Sequoia Union High School District agrees with the findings of the 2006-07 Grand Jury with regard to the need for privacy and security of student records. Attached is a copy of the District's Board Policy 5125, Student Records, Administrative Regulations 5125, Student Records, and Exhibit 5125, Students Records, which provides the technical standard to be followed in the District to ensure the security of student records.

Sincerely,

Patrick R. Gemma, Ed.D.
District Superintendent

cc: Board of Trustees

Student Records

The Board of Trustees recognizes the importance of keeping accurate, comprehensive student records as required by law. Procedures for maintaining the confidentiality of student records shall be consistent with state and federal law.

The Superintendent or designee shall establish regulations governing the identification, description and security of student records, as well as timely access for authorized persons. These regulations shall ensure parental rights to review, inspect and copy student records and shall protect the student and the student's family from invasion of privacy.

(cf. 3580 - District Records)
(cf. 4040 – Employee Use of Technology)
(cf. 5125.1 - Release of Directory Information)
(cf. 5125.2 - Withholding Grades, Diploma or Transcripts)
(cf. 5125.3 - Challenging Student Records)

The Superintendent or designee shall designate a certificated employee to serve as custodian of records, with responsibility for student records at the district level. At each school, the Principal or a certificated designee shall act as custodian of records for students enrolled at that school. The custodian of records shall be responsible for implementing board policy and administrative regulations regarding student records. (5 CCR 431)

Legal Reference:

EDUCATION CODE
48201 Student records for transfer students who have been suspended/expelled
48904 - 48904.3 Withholding grades, diplomas, or transcripts of pupils causing property damage or injury; transfer of pupils to new school districts; notice to rescind decision to withhold
48918 Rules governing expulsion procedures
49060-4907~~98~~ Pupil records
49091.14 Parental review of curriculum
CODE OF REGULATIONS, TITLE 5
430-438 Individual pupil records
16020-1602~~78~~ Destruction of records of school districts
GOVERNMENT CODE
6252-6260 Inspection of public records
FAMILY CODE
3025 Parental access to records
FEDERAL FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT OF 1974
20 U.S.C. 1232g
34 CODE OF FEDERAL REGULATIONS
99.1 - 99.67 Family Educational Rights and Privacy
300.500 Definition of "personally identifiable"
300.501 General responsibilities of public agencies
300.502 Opportunity to examine records
300.573 Destruction of information

STUDENT RECORDS

Definitions

Student records are any items of information gathered within or outside the district that are directly related to an identifiable student and maintained by the district or required to be maintained by an employee in the performance of his/her duties. Any information maintained for the purpose of second-party review is considered a student record. A student record may be recorded in handwriting, print, computer media, video or audio tape, film, microfilm, microfiche, or by other means. Student records include the student's health record. (Education Code 49061, 49062; 5 CCR 430; 34 CFR 99.3)

Student records do not include: (Education Code 49061, 49062; 5 CCR 430; 34 CFR 99.3)

1. Directory information

(cf. 5125.1 - Release of Directory Information)

2. Informal notes compiled by a school officer or employee which remain in the sole possession of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a substitute

3. Records of the law enforcement unit of the district, subject to the provisions of 34 CFR 99.8

(cf. 3515.3 - District Police/Security Department)

Mandatory permanent student records are those records which are maintained in perpetuity and which schools have been directed to compile by state law, regulation, or administrative directive. (5 CCR 430)

Mandatory interim student records are those records which the schools are directed to compile and maintain for stipulated periods of time and are then destroyed in accordance with state law, regulation, or administrative directive. (5 CCR 430)

Permitted student records are those records having clear importance only to the current educational process of the student. (5 CCR 430)

Access means a personal inspection and review of a record, an accurate copy of a record or receipt of an accurate copy of a record, an oral description or communication of a record, and a request to release a copy of any record. (Education Code 49061)

Disclosure means to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records, to any party, by any means including oral, written, or electronic means. (34 CFR 99.3)

Definitions (continued)

Personally identifiable information includes but is not limited to the student's name, the name of the student's parent/guardian or other family member, the address of the student or student's family, a personal identifier such as the student's social security number or student number, and a list of personal characteristics or other information that would make the student's identity easily traceable. (34 CFR 99.3)

Adult student is a person who is or was enrolled in school and who is at least 18 years of age. (5 CCR 430)

Parent/guardian means a natural parent, an adopted parent, or legal guardian. (Education Code 49061)

School officials and employees are officials or employees whose duties and responsibilities to the District, whether routine or as a result of special circumstances, require that they have access to student records.

A legitimate educational interest is one held by officials or employees whose duties and responsibilities to the district, whether routine or as a result of special circumstances, require that they have access to student records.

County placing agency means the county social service department or county probation department. (Education Code 49061)

Changes to Student Records

No additions except routine updating shall be made to a student's record after high school graduation or permanent departure without prior consent of the parent/guardian or adult student. (5 CCR 437)

Only a parent/guardian having legal custody of the student or an adult student may challenge the content of a record or offer a written response to a record. (Education Code 49061)

(cf. 5125.3 - Challenging Student Records)

Retention and Destruction of Student Records

All anecdotal information and assessment reports maintained as student records shall be dated and signed by the individual who originated the data. (5 CCR 431)

The following mandatory permanent student records shall be kept indefinitely: (5 CCR 432, 437)

1. Legal name of student
2. Date and place of birth and method of verifying birth date

Retention and Destruction of Student Records (continued)

(cf. 5111 - Admission)

3. Gender of student
4. Name and address of parent/guardian of minor student

    a. Address of minor student if different from the above

    b. Annual verification of parent/guardian's name and address and student's residence

(cf. 5111.1 - District Residency)
(cf. 5111.12 - Residency Based on Parent/Guardian Employment)
(cf. 5111.13 - Residency for Homeless Children)

5. Entrance and departure date of each school year and for any summer session or other extra session
6. Subjects taken during each year, half-year, summer session, or quarter, and marks or credits given

(cf. 5121 - Grades/Evaluation of Student Achievement)

7. Verification of or exemption from required immunizations

(cf. 5141.31 - Immunizations)

8. Date of high school graduation or equivalent

Mandatory interim student records, unless forwarded to another district, shall be maintained subject to destruction during the third school year following a determination that their usefulness has ceased or the student has left the District. These records include: (Education Code 48918, 51747; 5 CCR 432, 437, 16027)

1. Expulsion orders and the causes therefor

(cf. 5144.1 - Suspension and Expulsion/Due Process)
(cf. 5144.2 - Suspension and Expulsion/Due Process (Students with Disabilities))

2. A log identifying persons or agencies who request or receive information from the student record

3. Health information, including verification or waiver of the health screening for school entry

Retention and Destruction of Student Records (continued)

(cf. 5141.32 - Health Screening for School Entry)

4. Information on participation in special education programs, including required tests, case studies, authorizations, and evidence of eligibility for admission or discharge

(cf. 6159 - Individualized Education Program)
(cf. 6164.4 - Identification and Evaluation of Individuals for Special Education)

5. Language training records

(cf. 6174 - Education for English Language Learners)

6. Progress slips/notices required by Education Code 49066 and 49067

7. Parental restrictions/stipulations regarding access to directory information

8. Parent/guardian or adult student rejoinders to challenged records and to disciplinary action

9. Parent/guardian authorization or denial of student participation in specific programs

10. Results of standardized tests administered within the past three years

(cf. 6162.51 - Standardized Testing and Reporting Program)
(cf. 6162.52 - High School Exit Examination)

11. Written findings resulting from an evaluation conducted to determine whether it is in a student's best interest to remain in independent study

(cf. 6158 - Independent Study)

Permitted student records may be destroyed six months after the student completes or withdraws from the educational program, including: (5 CCR 432, 437)

1. Objective counselor/teacher ratings

2. Standardized test results older than three years

3. Routine disciplinary data

(cf. 5144 - Discipline)

4. Verified reports of relevant behavioral patterns

Retention and Destruction of Student Records (continued)

5. All disciplinary notices

6. Supplementary attendance records

Records shall be destroyed in a way that assures they will not be available to possible public inspection in the process of destruction. (5 CCR 437)

Persons Granted Access to Student Records Without Prior Written Consent

Persons, agencies, or organizations specifically granted access rights pursuant to law shall have access without prior written parental consent or judicial order. In addition, parental consent is not required when information is shared with other persons within educational institutions, agencies, or organizations obtaining access, as long as those persons have a legitimate educational interest in the information. (Education Code 49076)

The following persons or agencies shall have absolute access to any and all student records in accordance with law:

1. Parents/guardians of students younger than age 18 (Education Code 49069)

   Access to student records and information shall not be denied to a parent because he/she is not the child's custodial parent. (Family Code 3025)

2. An adult student age 18 or older or a student under the age of 18 who attends a postsecondary institution, in which case the student alone shall exercise rights related to his/her student records and grant consent for the release of records (34 CFR 99.5)

3. Any person, agency, or organization authorized in compliance with a court order or lawfully issued subpoena (Education Code 49077)

In addition, the following persons or agencies shall have access to those particular records that are relevant to the legitimate educational interest of the requester: (Education Code 49076)

1. Parents/guardians of a dependent student age 18 or older

2. Students age 16 or older or who have completed the 10th grade

3. School officials and district employees

4. Members of a school attendance review board and any volunteer aide age 18 or older who has been investigated, selected, and trained by such a board to provide follow-up services to a referred student

(cf. 5113.1 - Truancy)

Persons Granted Access to Student Records Without Prior Written Consent (continued)

5. Officials and employees of other public schools or school systems where the student intends or is directed to enroll, including local, county, or state correctional facilities where educational programs leading to high school graduation are provided

6. Federal, state, and local officials, as needed for program audits or compliance with law

7. Any district attorney who is participating in or conducting a truancy mediation program or participating in the presentation of evidence in a truancy petition

8. A prosecuting agency for consideration against a parent/guardian for failure to comply with compulsory education laws

9. Any probation officer or district attorney for the purposes of conducting a criminal investigation or an investigation in regards to declaring a person a ward of the court or involving a violation of a condition of probation

10. Any judge or probation officer for the purpose of conducting a truancy mediation program for a student, or for purposes of presenting evidence in a truancy petition pursuant to Welfare and Institutions Code 681

11. Any county placing agency for the purpose of fulfilling educational case management responsibilities required by the juvenile court or by law pursuant to Welfare and Institutions Code 16010 and to assist with the school transfer or enrollment of a student

(cf. 6173.1 - Education for Foster Youth)

Foster family agencies with jurisdiction over currently enrolled or former students may access those students' records of grades and transcripts, and any individualized education program (IEP) developed and maintained by the district with respect to such students. (Education Code 49069.3)

(cf. 6159 - Individualized Education Program)

When authorized by law to assist law enforcement in investigations of suspected kidnapping, the Superintendent or designee shall provide information about the identity and location of the student as it relates to the transfer of that student's records to any public school district or California private school.

The information shall be released only to designated peace officers, federal criminal investigators, and federal law enforcement officers whose names have been submitted in writing by their law enforcement agency in accordance with the procedures specified in Education Code 49076.5. (Education Code 49076.5)

The Superintendent or designee may release information from student records to the following: (Education Code 49076)

Persons Granted Access to Student Records Without Prior Written Consent (continued)

1. Appropriate persons in an emergency if the health and safety of a student or other persons are at stake

2. Accrediting associations

3. Under the conditions specified in Education Code 49076, organizations conducting studies on behalf of educational institutions or agencies for the purpose of developing, validating, or administering predictive tests, administering student aid programs, or improving instruction

4. Officials and employees of private schools or school systems where the student is enrolled or intends to enroll

5. Agencies or organizations in connection with a student's application for or receipt of financial aid

   However, information permitting the personal identification of a student or his/her parents/guardians for these purposes may be disclosed only as may be necessary to determine the eligibility of the student for financial aid, to determine the amount of financial aid, to determine the conditions which will be imposed regarding the financial aid, or to enforce the terms or conditions of the financial aid.

6. County elections officials for the purpose of identifying students eligible to register to vote and offering such students an opportunity to register

The Superintendent or designee may release a student's immunization record information to local health departments operating countywide or regional immunization information and reminder systems and the State Department of Health Services. The following information may be released: (Health and Safety Code 120440)

1. Name of the student and the student's parent/guardian
2. Student's gender
3. Student's date and place of birth
4. Types and dates of immunizations received
5. Manufacturer and lot number of the immunization received
6. Adverse reaction to the immunization
7. Other non-medical information necessary to establish the student's unique identity and record

STUDENT RECORDS

Access to Student Records with Prior Written Consent

Persons, agencies, or organizations not afforded access rights pursuant to law may be granted access only through written permission of the parent/guardian or adult student, or by judicial order. (Education Code 49075)

Only a parent/guardian having legal custody of the student may consent to the release of records to others. Either parent may grant consent if both parents notify the district, in writing, that such an agreement has been made. (Education Code 49061)

(cf. 5021 - Noncustodial Parents)

Any person or agency granted access is prohibited from releasing information to another person or agency without written permission from the parent/guardian or adult student. (Education Code 49076)

Procedures for Access

Student records shall be maintained in a central file at the school attended by the student or, when records are maintained in different locations, a notation shall be placed in the central file indicating where other records may be found. Parents/guardians shall be notified of the location of student records if not centrally located. (Education Code 49069; 5 CCR 433)

To inspect, review, or obtain copies of student records, authorized persons shall submit a request to the custodian of records.

Authorized persons, organizations, or agencies from outside the school whose access requires consent from the parent/guardian or adult student shall submit their request, together with any required authorization, to the Superintendent or designee or the custodian of records. (5 CCR 435)

When required by law, the parent/guardian shall provide a signed and dated written consent before the district discloses the student record. The consent shall specify the records that may be disclosed, state the purpose of the disclosure, and identify the party or class of parties to whom the disclosure may be made. Upon request by the parent/guardian, the District shall provide him/her a copy of the records disclosed. (34 CFR 99.30)

Within five days following the date of request, an authorized person shall be granted access to inspect, review, and obtain copies of student records during regular school hours. (Education Code 49069; 5 CCR 431)

Qualified certificated personnel shall be available to interpret records when requested. (Education Code 49069)

Procedures for Access (continued)

The custodian of records shall be responsible for the security of student records and shall assure that access is limited to authorized persons. (5 CCR 433) Specific standards for ensuring the security of electronic access to student information are available in E 5125, Acceptable Encryption Algorithm Standards.

The custodian of records or the Superintendent or designee shall prevent the alteration, damage, or loss of records during inspection. (5 CCR 435)

Prior to disclosing a record pursuant to a court order, the Superintendent or designee shall, unless otherwise instructed by the order, give the parent/guardian or adult student at least three days' notice of the name of the requesting agency and the specific record requested if lawfully possible within the requirements of the judicial order. (5 CCR 435)

When the District discloses personally identifiable information to officials of another school, school system, or postsecondary institution where the student seeks or intends to enroll, the Superintendent or designee shall make a reasonable attempt to notify the parent/guardian or adult student at his/her last known address, provide a copy of the record that was disclosed, and give him/her an opportunity for a hearing to challenge the record. (34 CFR 99.34)

Upon releasing student information to a judge or probation officer for the purpose of conducting a truancy mediation program or presenting evidence in a truancy petition, the Superintendent or designee shall inform, or provide written notification to, the student's parent/guardian within 24 hours. (Education Code 49076)

If the District is planning to release a student's immunization information to the county health department or state Department of Health Services, the Superintendent or designee shall inform the student's parents/guardians of the following: (Health and Safety Code 120440)

1. The type of information that will be shared

2. The name and address of the agency with which the district will share the information

3. That any shared information shall be treated as confidential and shall be used to share only with each other and, upon request, with health care providers, child care facilities, family child care homes, service providers for the Women, Infants and Children (WIC) food program, county welfare departments, foster care agencies, and health care plans

4. That the information may be used only to provide immunization service; to provide or facilitate third-party payer payments for immunizations; to compile and disseminate statistical information on immunization status on groups of people, without identifying the student

5. That the parent/guardian has the right to examine any immunization-related information shared in this manner and to correct any errors

Procedures for Access (continued)

6. That the parent/guardian may refuse to allow this information to be shared

Duplication of Student Records

To provide copies of any student record, the District shall charge a reasonable fee not to exceed the actual cost of furnishing the copies. No charge shall be made for providing up to two transcripts or up to two verifications of various records for any former student. No charge shall be made to locate or retrieve any student record. (Education Code 49065)

The Superintendent or designee shall set a fee and update the amount periodically if actual costs change.

(cf. 3260 - Fees and Charges)

Access Log

A log shall be maintained for each student's record which lists all persons, agencies, or organizations requesting or receiving information from the records and the legitimate educational interest of the requester. (Education Code 49064)

In every instance of inspection by persons who do not have assigned educational responsibility, the school custodian of records shall make an entry in the log indicating the record inspected, the name of the person granted access, the reason access was granted, and the time and circumstances of inspection. (5 CCR 435)

The log does not need to record access by: (Education Code 49064)

1. Parents/guardians or adult students

2. Students 16 years of age or older or who have completed the 10th grade

3. Parties obtaining district-approved directory information

(cf. 5125.1 - Release of Directory Information)

4. Parties who provide written parental consent, in which case the consent notice shall be filed with the record pursuant to Education Code 49075

5. School officials or employees who have a legitimate educational interest

The log shall be accessible only to the parent/guardian, adult student, dependent adult student, student age 16 years or older or who has completed the 10th grade, custodian of records, and certain state/federal officials. (Education Code 49064; 5 CCR 432)

STUDENT RECORDS

Transfer of Student Records

If a student transfers into this district from any other school district or a private school, the Superintendent or designee shall inform the parent/guardian of his/her rights regarding student records, including the right to review, challenge, and receive a copy of student records. (Education Code 49068; 5 CCR 438)

When a student transfers into this district from another, the Superintendent or designee shall request that the student's previous district provide any records, either maintained by that district in the ordinary course of business or received from a law enforcement agency, regarding acts committed by the transferring student that resulted in his/her suspension or expulsion. (Education Code 48201)

(cf. 4158/4258/4358 - Employee Security)

When a student transfers from this district to another school district or to a private school, the Superintendent or designee shall forward a copy of the student's mandatory permanent record as requested by the other district or private school. The original record or a copy shall be retained permanently by this district. If the transfer is to another California public school, the student's entire mandatory interim record shall be forwarded. If the transfer is out of state or to a private school, the mandatory interim record may be forwarded. Permitted student records may be forwarded to any other district or private school. (5 CCR 438)

Upon receiving a request from a county placing agency to transfer a student in foster care out of a district school, the Superintendent or designee shall transfer the student's records to the next educational placement within two business days. (Education Code 49069.5)

All student records shall be updated before they are transferred. (5 CCR 438)

Student records shall not be withheld from the requesting district because of any charges or fees owed by the student or parent/guardian. (5 CCR 438)

If the district is withholding grades, diploma, or transcripts from the student because of his/her damage or loss of school property, this information shall be sent to the requesting district along with the student's records.

(cf. 5125.2 - Withholding Grades, Diploma or Transcripts)

Notification of Parents/Guardians

Upon students' initial enrollment, and at the beginning of each year thereafter, the Superintendent or designee shall notify parents/guardians and eligible students, in writing, of their rights related to student records. Insofar as practicable, the district shall provide these notices in the student's home language and shall effectively notify parents/guardians or eligible students who are disabled. (Education Code 49063; 34 CFR 99.7)

(cf. 5145.6 - Parental Notifications)

STUDENT RECORDS

Notification of Parents/Guardians

The notice shall include: (Education Code 49063; 34 CFR 99.7, 99.34)

1. The types of student records kept by the district and the information contained therein

2. The title(s) of the official(s) responsible for maintaining each type of record

3. The location of the log identifying those who request information from the records

4. District criteria for defining "school officials and employees" and for determining "legitimate educational interest"

5. District policies for reviewing and expunging student records

6. The right to inspect and review student records, and the procedures for doing so

7. The right to challenge and the procedures for challenging the content of a student record that the parent/guardian or student believes to be inaccurate, misleading, or otherwise in violation of the student's privacy rights

(cf. 5125.3 - Challenging Student Records)

8. The cost, if any, charged for duplicating copies of records

9. The categories of information defined as directory information pursuant to Education Code 49073

10. The right to consent to disclosures of personally identifiable information contained in the student's records except when disclosure without consent is authorized by law

11. The availability of the curriculum prospectus developed pursuant to Education Code 49091.14 containing the titles, descriptions, and instructional aims of every course offered by the school

(cf. 5020 - Parent Rights and Responsibilities)

12. Any other rights and requirements set forth in Education Code 49060-49078, and the right of parents/guardians to file a complaint with the United States Department of Health, Education, and Welfare concerning an alleged failure by the district to comply with 20 USC 1232g

13. A statement that the District forwards education records to other agencies or institutions that have requested the records and in which the student seeks or intends to enroll

Acceptable Encryption Algorythm Standards

Purpose

The purpose of this exhibit to Board Policy 5125, Student Records, is to provide guidance which limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this exhibit provides direction to ensure that federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside the United States.

Scope

This exhibit applies to all Sequoia Union High School District employees and affiliates.

Guidelines

Proven, standard algorithms such as AES, Blowfish, RSA, RC5, and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Sequoia Union High School District's key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose. The export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

Enforcement

Any employee found to have violated these guidelines may be subject to disciplinary action, up to and including termination of employment.

Definitions

Proprietary Encryption is an algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Symmetric Cryptosystem is a method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem is a method of encryption in which two different keys are used: one for encrypting and one for decrypting the data, e.g., public-key encryption.

Application Service Provider Acquisition

Purpose

This document describes Information Security's guidelines for Application Service Providers (ASPs) that engage with the Sequoia Union High School District.

Scope

This guideline applies to any use of Application Service Providers by the Sequoia Union High School District, independent of where hosted.

Guidelines

Requirements of Project Sponsoring Organization

The ASP Sponsoring Organization must first establish that its project is an appropriate one for the ASP model, prior to engaging any additional infrastructure teams within the Sequoia Union High School District or ASPs external to the company. The person/team wanting to use the ASP service must confirm that the ASP chosen to host the application or project complies with this guideline. The Business Function to be outsourced must be evaluated against the following:

1. The requester must go through the ASP engagement process with the Information Services team to ensure affected parties are properly engaged.
2. In the event that the Sequoia Union High School District's data or applications are to be manipulated by, or hosted at, an ASP's service, the ASP sponsoring organization must have written, explicit permission from the data/application owners. A copy of this permission must be provided to Information Services.
3. The information to be hosted by an ASP must fall under the "Minimal Security" category. Information that is confidential may not be outsourced to an ASP. Refer to the *Information Sensitivity Policy* for additional details.
4. If the ASP provides confidential information to the Sequoia Union High School District, the ASP sponsoring organization is responsible for ensuring that any obligations of confidentiality are satisfied. This includes information contained in the ASP's application. Sequoia Union High School District's Administrative Services Division should be contacted for further legal guidance if questions about third-party data arise. Projects that do not meet these criteria may not be deployed to an ASP.

Requirements of the Application Service Provider

Information Services has created an associated document, entitled *ASP Security Standards* which sets forth the minimum security requirements for ASPs. The ASP must demonstrate compliance with these Standards in order to be considered for use.

The ASP engagement process includes an Information Services evaluation of security requirements. The *ASP Security Standards* can be provided to ASPs which are either being considered for use by the Sequoia Union High School District, or have already been selected for use.

Requirements of Project Sponsoring Organization

Requirements of the Application Service Provider (continued)

The Sequoia Union High School District may request that additional security measures be implemented in addition to the measures stated in the *ASP Security Standards* document, depending on the nature of the project.

The Sequoia Union High School District may change the requirements over time, and the ASP is expected to comply with these changes.

ASPs which do not meet these requirements, may not be used for Sequoia Union High School District projects.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Application Service Providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

Definitions

Application Service Providers (ASPs) combine hosted software, hardware and networking technologies to offer a service-based application, as opposed to a Sequoia District-owned and operated application. Common ASP offerings include enterprise resource planning (ERP), collaboration and sales force automation tools, but are not limited to these things.

ASP Sponsoring Organization is the group within the Sequoia Union High School District which wishes to utilize the services of an ASP.

Business Function is the business need which a software application satisfies. It is managed by an ASP which hosts an application on behalf of the Sequoia Union High School District.

Application Service Provider (ASP) Security Standards

Overview

This guideline defines the minimum security criteria that an Application Service Provider (ASP) must meet in order to be considered for use by the Sequoia Union High School District. As part of the ASP selection process, the ASP Vendor must demonstrate compliance with the Standards listed below by responding in writing to EVERY statement and question in the six categories. Information Services will closely review the vendor responses, and will suggest remediation measures in any areas that fall short of the minimum security criteria. The Sequoia Union High School District's approval of any given ASP resides largely on the vendor's response to this document.

Requirements of Project Sponsoring Organization (continued)

Scope

This guideline can be provided to ASPs which are either being considered for use by the Sequoia Union High School District or have already been selected for use.

Responding to These Standards

The Sequoia Union High School District is looking for explicitly detailed, technical responses to the following statements and questions. ASPs should format their responses directly beneath the Standards (both questions and requirements) listed below. In addition, any security whitepapers, technical documents, or policies which may address a guideline must be included and must be specific and avoid generalities.

Examples:

- Bad: "We have hardened our hosts against attack."
- Good: "We have applied all security patches for Windows 2000 as of August 31, 2000, to our servers. Our Administrator is tasked with keeping up-to-date on current vulnerabilities that may affect our environment, and our policy is to apply new patches during our maintenance period (2300hrs, Saturday) every week. Critical updates are implemented within 24 hours. A complete list of applied patches is available to the Sequoia Union High School District."
- Bad: "We use encryption."
- Good: "All communications between our site and <Company Name> will be protected by IPSec ESP Tunnel mode using 168-bit TripleDES encryption, SHA-1 authentication. We exchange authentication material via either out-of-band shared secret or PKI certificates."

Standards

General Security

5. The Sequoia Union High School District reserves the right to periodically audit the Application Service Provider's application infrastructure to ensure compliance with the ASP Guideliens and these Standards. Non-intrusive network audits, i.e., basic portscans, etc., may be done randomly, without prior notice. More intrusive network and physical audits may be conducted on site with 24 hours notice.

6. The ASP must provide a proposed architecture document which includes a full network diagram of the Sequoia Union High School District's Hosted Application Environment, illustrating the relationship between the Environment and any other relevant networks, with a full data flowchart which details where the Sequoia Union High School District's data resides, the applications that manipulate it, and the security thereof.

Requirements of Project Sponsoring Organization

General Security (continued)

7. The ASP must be able to immediately disable all or part of the functionality of the application should a security issue be identified.

Physical Security

1. The equipment hosting the application for the Sequoia Union High School District must be located in a physically secure facility, which requires badge access at a minimum.

2. The infrastructure (hosts, network equipment, etc.) hosting the Sequoia Union High School District's application must be located in a locked cage-type environment.

3. The Sequoia Union High School District shall have final say on who is authorized to enter any locked physical environment, as well as to access the Sequoia Union High School District's Application Infrastructure.

4. The ASP must disclose who amongst their personnel will have access to the environment hosting the application for the Sequoia Union High School District.

5. The Sequoia Union High School District requires that the ASP disclose its ASP background check procedures and results prior to any approval for use of an ASP-hosted service.

Network Security

1. The network hosting the application must be air-gapped from any other network or customer that the ASP may have. This means the Sequoia Union High School District's application environment must use separate hosts and separate infrastructure.

2. Data transmission will be facilitated between the Sequoia Union High School District and the ASP in the following two things:

    a. If the Sequoia Union High School District will be connecting to the ASP via a private circuit (such as frame relay, etc.), that circuit must terminate on the Sequoia District extranet, and the operation of that circuit will come under the procedures and guidelines that govern the Sequoia Union High School District.

    b. If, on the other hand, the data between the Sequoia Union High School District and the ASP will go over a public network such as the Internet, appropriate firewalling technology must be deployed by the ASP, and the traffic between Sequoia Union High School District and the ASP must be protected and authenticated by cryptographic technology (See Cryptography below).

Requirements of Project Sponsoring Organization (continued)

Host Security

1. The ASP must disclose how and to what extent the hosts (Unix, Linux, NT, etc.) comprising the Sequoia Union High School District application infrastructure have been hardened against attack. If the ASP has hardening documentation for the CAI, provide that as well.

2. The ASP must provide a listing of current patches on hosts, including host OS patches, web servers, databases, and any other material application.

3. Information on how and when security patches will be applied must be provided. How does the ASP keep up on security vulnerabilities, and what is the policy for applying security patches?

4. The ASP must disclose its processes for monitoring the integrity and availability of those hosts.

5. The ASP must provide information on its password policy for the Sequoia Union High School District application infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.

6. The Sequoia Union High School District cannot provide internal usernames/passwords for account generation, as the company is not comfortable with internal passwords being in the hands of third parties. With that restriction, how will the ASP authenticate users? For example, LDAP, Client certificates, Kerberos, etc.

7. The ASP must provide information on the account generation, maintenance, and termination process, for both maintenance as well as user accounts. Include information as to how an account is created, how account information is transmitted back to the user, and how accounts are terminated when no longer needed.

Web Security

1. At the Sequoia Union High School District's discretion, the ASP may be required to disclose the specific configuration files for any web servers and associated support functions (such as search engines or databases).

2. Whether and where the application uses any dynamic page generation technology, such as Java, Javascript, ActiveX, PHP or ASP (active server page), technology must be disclosed.

3. The language the application is back-end written in (C, Perl, Python, VBScript, PHP, etc.) must be disclosed.

4. The ASP process for doing security Quality Assurance testing for the application must be included. For example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture.

Requirements of Project Sponsoring Organization

Web Security (continued)

5. The ASP must include whether it has done web code review, including CGI, Java, etc, for the explicit purposes of finding and remediating security vulnerabilities. If so, who performed the review, the results, and what remediation activity took place must be included If not, disclose when such an activity is planned.

Cryptography

1. The Sequoia Union High School District application infrastructure cannot and will not utilize any "homegrown" cryptography. Any symmetric, asymmetric or hashing algorithm utilized by the ASP must utilize algorithms that have been published and evaluated by the general cryptographic community.

2. Encryption algorithms must be of sufficient strength to equate to 128-bit AES.

3. Preferred hashing functions are SHA-1 and MD-5.

4. Connections to the ASP utilizing the Internet must be protected using any of the following cryptographic technologies: IPSec, SSL, SSH/SCP, PGP, AES (with a key length of 128 bits or greater).

5. If the ASP application infrastructure requires PKI, please contact the Sequoia Union High School District for additional guidance.

Prohibition Against Automatic Forwarding of Electronic Mail

Purpose

To prevent the unauthorized or inadvertent disclosure of sensitive district information.

Scope

These guidelines cover automatic email forwarding and, thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of the Sequoia Union High School District.

Guidelines

Employees must exercise the utmost caution when sending any email from inside the Sequoia Union High School District to an outside network. Sequoia Union High School District email will not be automatically forwarded to an external destination. Sensitive information, as defined in the *Information Sensitivity Policy*, will not be forwarded via any means, unless that email is critical to business and is encrypted in accordance with the *Acceptable Encryption Policy*.

Prohibition Against Automatic Forwarding of Electronic Mail (continued)

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Email is the electronic transmission of information through a mail protocol such as SMTP Programs. Novell Groupwise, Eudora, and Microsoft Outlook use SMTP.

Forwarded email is the email resent from internal networking to an outside point.

Sensitive information is information considered sensitive if it contains "personal information," as defined in the Information Sensitivity Guidelines.

Unauthorized Disclosure is the intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

Virtual Private Network (Vpn) Access Guidelines

Purpose

The following are guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the Sequoia Union High School District network.

Scope

This guideline applies to all Sequoia Union High School District employees, contractors, consultants, temporaries, and other workers, including all personnel affiliated with third parties utilizing VPNs to access the Sequoia Union High School District network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

Guideline

Approved Sequoia Union High School District employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Guidelines.*

Additionally:

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Sequoia Union High School District's internal networks.

2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

Virtual Private Network (Vpn) Access Guidelines

Guideline (continued)

3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.

5. VPN gateways will be set up and managed by Sequoia Union High School District's network operational groups.

6. All computers connected to Sequoia Union High School District's internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard; this includes personal computers.

7. VPN users will be automatically disconnected from the Sequoia Union High School District's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

8. The VPN concentrator is limited to an absolute connection time of 24 hours.

9. Users of computers that are not District-owned equipment must configure the equipment to comply with Sequoia Union High School District's VPN and network policies.

10. Only VPN clients which have been approved by Technology and Information Services may be used.

11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the Sequoia Union High School District's network, and as such are subject to the same rules and regulations that apply to District-owned equipment, i.e., their machines must be configured to comply with Sequoia Union's Security Guidelines.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Wireless Networking Guideline

Purpose

This guideline prohibits access to the Sequoia Union High School District networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by the Assistant Superintendent of Administrative Services are approved for connectivity to the Sequoia Union High School District's networks.

Wireless Networking Guideline (continued)

Scope

This guideline covers all wireless data communication devices, e.g., personal computers, cellular phones, PDAs, etc., connected to any of the Sequoia Union High School District's internal networks which transmit or host confidential data or administrative applications. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to the Sequoia Union High School District's networks do not fall under the purview of this guideline.

Guideline

Register Access Points and Cards

All wireless Access Points/Base Stations connected to the district network must be registered and approved by Technology and Information Services. These Access Points/Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards, i.e., PC cards, used in district laptop or desktop computers must be registered with Technology, and this list must be provided to Information Services on a periodic basis.

Approved Technology

All wireless LAN access must use District-approved vendor products and security configurations (see Encryption Guideline).

VPN Encryption and Authentication

All computers with wireless LAN devices must utilize a District-approved Virtual Private Network (VPN) (see Virtual Private Network guideline) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 128 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS, or something similar.

Setting the SSID

The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

User Authentication is a method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

Password Protection and Use Guideline

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Sequoia Union High School District's entire network. As such, all Sequoia Union High School District employees (including contractors, vendors, and third parties with access to Sequoia Union High School District systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Sequoia Union High School District facility, has access to the Sequoia Union High School District network, or stores any confidential information.

General

1. All system-level passwords, e.g., root, enable, NT admin, application administration accounts, etc., must be changed on at least a quarterly basis.

2. All production system-level passwords must be part of the Technology and Information Services administered global password management database.

3. All user-level passwords, e.g., email, web, desktop computer, etc., must be changed at least every six months. The recommended change interval is every four months.

4. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

5. Passwords must not be inserted into email messages or other forms of electronic communication.

6. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private," and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used, e.g., SNMPv2 or SNMPv3.

7. All user-level and system-level passwords must conform to the guidelines described below.

General Password Construction Guidelines

Passwords are used for various purposes at the Sequoia Union High School District. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens, i.e., dynamic passwords, which are only used once, everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

1. The password contains less than eight characters

2. The password is a word found in a dictionary (English or foreign)

3. The password is a common usage word such as:

    a. Names of family, pets, friends, co-workers, fantasy characters, etc.
    b. Computer terms and names, commands, sites, companies, hardware, software.
    c. The words "SUHSD," "sanjose," "sanfran," or any derivation.
    d. Birthdays and other personal information such as addresses and phone numbers.
    e. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    f. Any of the above spelled backwards.
    g. Any of the above preceded or followed by a digit, e.g., secret1, 1secret.

Strong passwords have the following characteristics:

1. Contain both upper and lower case characters, e.g., a-z, A-Z.

2. Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

3. Are at least eight alphanumeric characters long.

4. Are not a word in any language, slang, dialect, jargon, etc.

5. Are not based on personal information, names of family, etc.

6. Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. NOTE: Do not use either of these examples as passwords!

Password Protection Standards

The same password for Sequoia Union High School District accounts should not be used for other non-Sequoia Union High School District access, e.g., personal ISP account, option trading, benefits, etc. Where possible, the same password for various Sequoia Union High School District access needs should not be used. For example, select one password for the Student Information System and a separate password for general e-mail login.

Password Protection Standards (continued)

Sequoia Union High School District passwords should not be shared with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Sequoia Union High School District-Owned Information.

Don't:

- Reveal a password over the phone to ANYONE.
- Reveal a password in an email message
- Reveal a password to the boss.
- Talk about a password in front of others.
- Hint at the format of a password, e.g., "my family name."
- Reveal a password on questionnaires or security forms.
- Share a password with family members.
- Reveal a password to co-workers while on vacation.

If a password is demanded, the person should be referred to these guidelines or to the Information Services Department.

The "Remember Password" feature of applications, e.g., Eudora, OutLook, Netscape, Firefox, Internet Explorer, Thunderbird, Microsoft Windows, Mac OS X, Gnome, etc., should not be used.

Passwords must not be written down or stored in the office. Passwords must not be stored in a file on ANY computer system, including Palm Pilots or similar devices, without encryption meeting the standards of the Sequoia Union High School District's Encryption Policy.

Change passwords at least once every six months, except system-level passwords, which must be changed quarterly. The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to Information Services and change all passwords immediately.

Password cracking or guessing may be performed on a periodic or random basis by Information Services or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications should:

- authenticate individual users, not groups
- not store passwords in clear text or in any easily reversible form
- provide for some sort of role management, i.e., one user can take over the functions of another without having to know the other's password
- support TACACS+, RADIUS, and/or X.509 with LDAP security retrieval, wherever possible.

STUDENT RECORDS

Use of Passwords and Passphrases for Remote Access Users

Access to the Sequoia Union High School District's networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase is:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

The previous rules that apply to passwords apply to passphrases.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Application Administration Account is any account that is for the administration of an application, e.g., Oracle database administrator, MSSQL SA user, ISSU administrator, etc.

THE FOLLOWING PAGES ARE
PROVIDED FOR EMPLOYEE FOR SIGNATURE

EMPLOYEE INFORMATION SECURITY GUIDELINE
INFORMATION SENSITIVITY POLICY AND LEGAL DEFINITIONS

Overview

The Sequoia Union High School District permits access to administrative systems and/or paper or electronic documents containing confidential data to approved employees. The purpose of this access is to better enable approved employees to process work and meet deadlines. It is the responsibility of Sequoia Union High School District employees accessing administrative applications to maintain the security of this information by following all Sequoia Union High School District policies, procedures, and guidelines and abiding by all applicable privacy laws and regulations as stated below and elsewhere in the Sequoia Union High School District's board policies, administrative regulations, exhibits, and posted procedures. It is equally important for Sequoia Union High School District employees transporting equipment and/or documents containing personal or confidential data to maintain the security of this information at all times. Failure to abide by these policies, procedures, guidelines, and laws may result in the loss of access to Sequoia Union High School District's systems and/or legal consequences (criminal and/or civil).

Scope

For the purposes of this guideline, Sequoia Union High School District administrative systems will include, but not be limited to, any student information system, special education system, business and/or financial information system, personnel/human resource systems, or any system which processes or stores information related to individual students, employees, or their family members.

Applicable Laws and Regulations

California Penal Code, Section 502 – Unauthorized Access to Computers, Computer Systems, and Computer Data:

This section provides that any person who commits one of the acts listed below is guilty of a public offense. The Sequoia Union High School District considers any use of Sequoia Union High School District computer systems or access to any Sequoia Union High School District-owned data containing confidential information with the intent to commit one of the listed offenses to be "without permission". Listed offenses include, but are not limited to:

1. Damaging, deleting, destroying, or using any data to defraud, deceive, extort or wrongfully control or obtain money, property or data.
    1. Using computer services without permission.
    2. Assisting unauthorized persons in the use of computer services without permission.
    3. Assisting unauthorized persons in gaining access to documents containing personal data without permission.
    4. Altering, deleting, adding or destroying printed ("hard copy") documents or electronic data on Sequoia Union High School District systems without permission.
    5. Disrupting computer services or causing the denial of computer services to an authorized user.
    6. Knowingly introducing any malicious program or computer contaminant into any computer, computer system or computer network.
    7. Bypassing any Sequoia Union High School District security system in order to facilitate the unauthorized transmission of data across the Sequoia Union High School District Network, or to disable or make unauthorized modifications to any Sequoia Union High School District security system.

The Sequoia Union High School District is obligated to, and will, report all violations of the above section to the appropriate authorities, which may lead to, but is not limited to, fines of up to $10,000 and/or imprisonment of up to three years.

3.2 California Civil Code Section 1798.80-1798.84: The Definition of Personal Information/Confidential Information.

For the purposes of this document, Personal Information and Confidential Information have the same definition, and may be used interchangeably.

1. “Personal Information” means an individual's first name or initial and his or her last name in combination with any one or more of the following data elements, when either the name or data elements are not encrypted or redacted:

   a) Social security number
   b) Driver's license number or California identification card number
   c) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
   d) Medical information

2. “Medical Information” means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional.

3. “Personal Information” does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

3.3 Information Considered Confidential by the Sequoia Union High School District

Any personally identifiable data in a student information system, special education system, business and/or financial information system, personnel/human resource systems, or any system which processes or stores information related to individual students, employees, or their family members is considered confidential and may not be provided to any unauthorized third party.

TERMS AND CONDITIONS FOR REMOTE ACCESS TO SEQUOIA UNION HIGH SCHOOL DISTRICT'S NETWORK ("REMOTE ACCESS POLICY")

TO BE SIGNED BY EMPLOYEES

Off site access to any Sequoia Union High School District network hosting administrative systems or transporting confidential information is/are subject to the following conditions:

1. Employees requesting off-site access to Sequoia Union High School District networks hosting administrative systems or confidential data must sign and adhere to the rules and policy as stated in this document.

2. Off-site access to Sequoia Union High School District networks hosting administrative systems or confidential data requires the written authorization of the Assistant Superintendent for Business Services. A copy of the written authorization is to be kept on file by Information Services for a period of two years.

3. Off-site access to Sequoia Union High School District networks which host administrative applications or confidential data is limited to secured channels as established and configured by the Sequoia Union High School District's Technology and Information Services department (please see the "VPN Access Policy" and "Wireless Access Policy").

4. Off-site access to Sequoia Union administrative systems is limited to Sequoia Union High School District owned equipment, unless otherwise authorized in writing by the Assistant Superintendent of Business Services. The equipment are to be automatically scanned to viruses and other malicious programs that could compromise the integrity of the Sequoia Union High School District's network security. Remote users understand that their machines are a de facto extension of the Sequoia Union High School District's network, and as such are subject to the same rules and regulations that apply to Sequoia Union-owned equipment, i.e., their machines must be configured to comply with Sequoia Union's Security Policies.

5. All equipment used to remotely access the Sequoia Union High School District network must be inspected annually by Technology and Information Services for the presence of malicious programs, applications not authorized or owned by the Sequoia Union High School District, or any other program or application which could compromise the integrity of the Sequoia Union High School District's network.

6. No user shall allow any non-authorized person to access any machine connected to the Sequoia Union High School District network for any reason at any time. Passwords are not to be shared at any time.

7. Remote access to the Sequoia Union High School District network is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase. Access to individual administrative applications must be password protected. All administrative applications must time out within a 30 minute period of inactivity and can only be re-accessed with a password. No personally owned software is to be installed on a Sequoia Union High School District-owned computer.

8. Remote users of the Sequoia Union High School District network are not to print off-site any screen capture, report or other hard-copy documents that contain personal or confidential information regarding any Sequoia Union High School District student, staff member, or a family member of any Sequoia Union High School District student or staff member.

9. Remote users, or any user utilizing a portable device , i.e., laptop or portable storage medium, i.e., removable hard drive, “IPOD,” etc., shall not save any data containing confidential or personal information, including but not limited to any information pertaining to Sequoia Union High School District students, staff members, or family members of any Sequoia Union High School District students or staff members to the portable laptop or storage medium.

10. Personal data as defined in the Information Sensitivity Policy and/or California Civil Code Section 1798.80-1798.84 that is transported electronically or physically shall not be saved on any personally owned storage device or computer, even if the data is to be stored temporarily.

11. Employees must return Sequoia Union High School District equipment, including portable media, when on a leave of absence. Upon separation of employment, employees must immediately return all Sequoia Union High School District equipment. The Sequoia Union High School District retains the right to withhold the employee's final paycheck until all Sequoia Union High School District equipment has been returned.

12. All users must report a systems security breach to Information Services immediately upon discovery.

13. The Sequoia Union High School District maintains the right to monitor all activity involving Sequoia Union High School District networks and administrative systems and any time without prior notice.

14. The Sequoia Union High School District retains the right to terminate access to any Sequoia Union High School District system at any time without prior notice.

15. All data collected, printed and/or stored on any device owned or leased by the Sequoia Union High School District is the property of the Sequoia Union High School District.

16. The Sequoia Union High School District retains the right to amend its policy and/or rules at any time without prior notice.

17. Employees understand that they will be held liable for any financial damages resulting from their illegal use of the Sequoia Union High School District's computer network and/or it's administrative applications.

ACCEPTABLE USE POLICY ACKNOWLEDGEMENT

I, _____ (print first and last name), have read and understand the above Terms and Conditions of Use and agree to abide by them. I further understand that any violations of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, I may be subject to disciplinary action, from termination of technology access privileges up to termination of employment. Appropriate legal action may also be taken.

Signature of User: _____ Date: _____

Name (print): _____