Policy Committee Meeting

NOTICE IS HEREBY GIVEN that a meeting of the Policy Committee Meeting of the Governing Board of the Texas School for the Deaf shall be held on **February 20, 2020** at **12:00 PM**, Texas School for the Deaf, Multipurpose Room of the Ford/CTE Bldg 1102 South Congress Ave Austin, Tx 78704.

If, during the course of the meetings, any discussion of any item on the agenda should be held in closed meeting, the Committee shall convene in such closed meeting in accordance with Texas Government Code, Sec. 551.001, et seq. Before any such session is convened, the presiding officer shall publicly identify the section or sections of the Code authorizing the closed meeting. All final votes, actions, or decisions shall be taken in open session.

The subjects to be discussed or considered, or upon which any formal action may be taken, are as follows (items do not have to be taken in the same order as shown on this meeting notice):

AGENDA

1. **Call to Order**
2. **December 12th, 2019 Meeting Minutes** (Sha Cowan)
3. **Review Board Policies** (Sha Cowan)
   A. **FFBA** - (NEW) Crisis Intervention: Trauma Informed Care
   B. **FFB** - (NEW) Student Welfare - Crisis Intervention
   C. **CQB** - Cybersecurity
4. **Adjournment**

Policy Committee
December 12, 2019
Meeting Minutes

Sha Cowan, Committee Chair
Members: Shawn Saladin, David Saunders, Heather Withrow

Call to Order

A Policy Committee Meeting of the Texas School for the Deaf was held at the Texas School for the Deaf campus, in Austin Texas on December 12, 2019. The meeting was called to order by Board President Eric Hogue sitting in for Committee Chair Sha Cowan at 3:16 pm, Board President Eric Hogue presiding. Committee members: David Saunders, and Heather Withrow were in attendance.

Approval of Minutes

The October 18, 2019 minutes were motioned by David Saunders to be accepted as is. Heather Withrow seconded the motion. All were in favor of accepting the October 18, 2019 meeting minutes as is. Motion carries unanimously.

Policy Review and Approval

DBA Employment Requirements and Restrictions: Credentials and Records
DEC Compensation and Benefits: Leaves and Absences
DFAC Probationary Contracts: Return to Probationary Status
DHE Employee Standards of Conduct: Searches and Alcohol Drug Testing
GNB Relations with Educational Entities: Regional Education Service Centers
GNC Community Relations: Colleges and Universities
FO Student Discipline
FOF Students Discipline: Students with Disabilities
EHBD Special Programs: Federal Title I
EHDB (NEW) Alternative Methods for Earning Credit: Credit by Examination with Prior Instruction
EHDC (NEW) Alternative Methods for Earning Credit: Credit by Examination without Prior Instruction
EHAB Basic Instructional Program: Required Instruction: Elementary
EHBF Special Programs: Career and Technical Education
EMI Miscellaneous Instructional Policies: Study of Religion
GKA (EXHIBIT) Community Relations: Conduct on School Premises

The above polices were motioned by Heather Withrow to be accepted as is. David Saunders seconded the motion. All were in favor of accepting the above policies as is. Motion carries unanimously.

GND Relations with Educational Entities: State Education Agency
FOE Student Discipline: Emergency and Alternative Placement
FOB Student Discipline: Out of School Suspension
FOD Student Discipline: Expulsion
EFA Instructional Resource: Instructional Materials

The above policies were motioned by Heather Withrow to be accepted with minor changes. David Saunders seconded the motion. All were in favor of accepting the policies with minor changes. Motion carries unanimously.

EEJA (DELETE) Individualized Learning: Credit by Examination with Prior Instruction
EEJB (DELETE) Individualized Learning: Credit by Examination without Prior Instruction
EFAA (DELETE) Instructional Materials: Selection and Adoption

The above policies were motioned by Heather Withrow to be deleted. David Saunders seconded the motion. All were in deleting the above policies. Motion carries unanimously.

Adjournment
Board President Eric Hogue substituting for Committee Chair Sha Cowan adjourned The Texas School for the Deaf Policy Committee meeting at 4:57 pm.

Trauma-Informed Care Policy

The School shall adopt and implement a policy requiring the integration of trauma-informed practices in the school environment. The School must include the policy in the School improvement plan required under Education Code 11.252 [see BQ].

The policy must address:

1. Using resources developed by the Texas Education Agency (TEA), methods for:

   a. Increasing staff and parent awareness of trauma-informed care; and

   b. Implementation of trauma-informed practices and care by School and campus staff; and

2. Available counseling options for students affected by trauma or grief.

Education Code 38.036(a)–(b)

Training

The methods for increasing awareness and implementation of trauma-informed care must include training as provided below. The training must be provided:

1. Through a program selected from the list of recommended best practice-based programs and research-based practices established under Health and Safety Code 161.325; The program must include mental health promotion and intervention, substance abuse prevention and intervention, and suicide prevention, that:

   (1) include a procedure for providing educational material to all parents and families in the School that contains information on identifying risk factors, accessing resources for treatment or support provided on and off campus, and accessing available student accommodations provided on campus;

   (2) include a procedure for providing notice of a recommendation for early mental health or substance abuse intervention regarding a student to a parent or guardian of the student within a reasonable amount of time after the identification of early warning signs as described by Subsection (b)(2);

   (3) include a procedure for providing notice of a student identified as at risk of committing suicide to

a parent or guardian of the student within a reasonable amount of time after the identification of early warning signs as described by Subsection (b)(2);

(4) establish that the School may develop a reporting mechanism and may designate at least one person to act as a liaison officer in the School for the purposes of identifying students in need of early mental health or substance abuse intervention or suicide prevention; and

(5) set out available counseling alternatives for a parent or guardian to consider when their child is identified as possibly being in need of early mental health or substance abuse intervention or suicide prevention.

2. As part of any new employee orientation for all new School educators; and

3. To existing School educators on a schedule adopted by TEA that requires educators to be trained at intervals necessary to keep educators informed of developments in the field.

For any training under this provision, the School shall maintain records that include the name of each staff member who participated in the training.

If the School determines that the School does not have sufficient resources to provide the training required under this provision, the School may partner with a community mental health organization to provide training that meets the requirements at no cost to the School.

Education Code 38.036(c)–(d), (f)

Reporting to TEA

The School shall report annually to TEA the following information for the school as a whole:

1. The number of teachers, principals, and counselors employed by the School who have completed training under this provision; and

2. The total number of teachers, principals, and counselors employed by the School.

Education Code 38.036(e)

Threat Assessment

Definitions

"Harmful, threatening, or violent behavior" includes behaviors, such as verbal threats, threats of self harm, bullying, cyberbullying, fighting, the use or possession of a weapon, sexual assault, sexual harassment, dating violence, stalking, or assault, by a student that could result in:

1. Specific interventions, including mental health or behavioral supports;
2. In-school suspension;
3. Out-of-school suspension; or
4. The student's expulsion or removal to a disciplinary alternative education program (DAEP).

"Team" means a threat assessment and safe and supportive school team established by the board under Education Code 37.115.

Education Code 37.115(a)

Threat Assessment Team

The board shall establish a threat assessment and safe and supportive school team to serve at the School and shall adopt policies and procedures for the teams.

The team is responsible for developing and implementing the safe and supportive school program in compliance with Texas Education Agency (TEA) rules at the School served by the team.

The policies and procedures adopted under Education Code 37.115 must:

1. Be consistent with the model policies and procedures developed by the Texas School Safety Center (TxSSC) [see Education Code 37.220];
2. Require each team to complete training provided by the TxSSC or a regional education service center (ESC) regarding evidence-based threat assessment programs; and
3. Require each team established under this section to report the required information regarding the team's activities to TEA [see Reporting to TEA, below].

Membership

The superintendent shall ensure that the members appointed to each team have expertise in counseling, behavior management, mental health and substance use, classroom instruction, special education, school administration, school safety and security, emergency management, and law enforcement.

Oversight Committee

The superintendent may establish a committee, or assign to an existing committee established by the School, the duty to oversee the operations of teams established for the School. A committee with oversight responsibility must include members with expertise in human resources, education, special education, counseling, behavior management, school administration, mental health and substance use, school safety and security, emergency management, and law enforcement.

Team Duties

Each team shall:

1. Conduct a threat assessment that includes assessing and reporting individuals who make threats of violence or exhibit harmful, threatening, or violent behavior in accordance with School policies and procedures; and gathering and analyzing data to determine the level of risk and appropriate intervention, including:
    a. Referring a student for mental health assessment; and
    b. Implementing an escalation procedure, if appropriate, based on the team's assessment, in accordance with School policy;
2. Provide guidance to students and school employees on recognizing harmful, threatening, or violent behavior that may pose a threat to the community, school, or individual; and
3. Support the School in implementing the School's multihazard emergency operations plan [see CKC].

Consent for Mental Health-Care Service

A team may not provide a mental health-care service to a student who is under 18 years of age unless the team obtains written consent from the parent of or the person standing in parental relation to the student before providing the mental health-care service. The consent must be submitted on a form developed by the School that complies with all applicable state and federal law. The student's parent or person standing in parental relation to the student may give consent for a student to receive ongoing services or may limit consent to one or more services provided on a single occasion.

Education Code 37.115(d)–(g)

Determination of Risk

On determination that a student or other individual poses a serious risk of violence to self or others, a team shall immediately report the team's determination to the superintendent. If the individual is a student, the superintendent shall immediately attempt to inform the parent or person standing in parental relation to the student. These requirements do not prevent an employee of the school from acting

immediately to prevent an imminent threat or respond to an emergency.

A team identifying a student at risk of suicide shall act in accordance with the School's suicide prevention program. If the student at risk of suicide also makes a threat of violence to others, the team shall conduct a threat assessment in addition to actions taken in accordance with the School's suicide prevention program.

A team identifying a student using or possessing tobacco, drugs, or alcohol shall act in accordance with School policies and procedures related to substance use prevention and intervention.

Education Code 37.115(h)–(j)

Reporting to TEA

A team must report to TEA in accordance with TEA-developed guidelines the following information regarding the team's activities and other information for the campus the team serves:

1. The occupation of each person appointed to the team;
2. The number of threats and description of the type of threats reported to the team;
3. The outcome of each assessment made by the team, including:
    a. Any disciplinary action taken, including a change in school placement;
    b. Any action taken by law enforcement; or
    c. A referral to or change in counseling, mental health, special education, or other services;
4. The total number, disaggregated by student gender, race, and status as receiving special education services, being at risk of dropping out of school, being in foster care, experiencing homelessness, being a dependent of military personnel, being pregnant or a parent, having limited English proficiency, or being a migratory child, of, in connection with an assessment or reported threat by the team:
    a. Citations issued for Class C misdemeanor offenses;
    b. Arrests;
    c. Incidents of uses of restraint;
    d. Changes in school placement, including placement in a JJAEP or DAEP;

e. Referrals to or changes in counseling, mental health, special education, or other services;

f. Placements in in-school suspension or out-of-school suspension and incidents of expulsion;

g. Unexcused absences of 15 or more days during the school year; and

h. Referrals to juvenile court for truancy; and

5. The number and percentage of school personnel trained in:

a. A best-practices program or research-based practice under Health and Safety Code 161.325, including the number and percentage of school personnel trained in suicide prevention or grief and trauma-informed practices;

b. Mental health or psychological first aid for schools;

c. Training relating to the safe and supportive school program; or

d. Any other program relating to safety identified by the commissioner.

Education Code 37.115(k)

Recommended Programs

The Texas Department of State Health Services (TDSHS), in coordination with TEA and ESCs, shall provide and annually update a list of recommended best practice-based programs and research-based practices in the areas specified below for implementation in public elementary, junior high, middle, and high schools within the general education setting. The School may select from the list a program or programs appropriate for implementation in the School.

Subject Areas

The list must include programs and practices in the following areas:

1. Early mental health intervention;

2. Mental health promotion;

3. Building skills related to managing emotions, establishing and maintaining positive relationships, and responsible decision-making;

4. Substance abuse prevention and intervention;

5. Suicide prevention;

6. Grief-informed and trauma-informed practices;

7. Positive behavior interventions and supports and positive youth development; and

8. Safe, supportive, and positive school climate.

"School climate" means the quality and character of school life, including interpersonal relationships, teaching and learning practices, and organizational structures, as experienced by students enrolled in the School, parents of those students, and personnel employed by the School.

TDSHS, TEA, and each ESC shall make the list easily accessible on their websites.

Practices and Procedures

The School may develop practices and procedures concerning each area listed above, including mental health promotion and intervention, substance abuse prevention and intervention, and suicide prevention, that:

1. Include a procedure for providing educational material to all parents and families in the School that contains information on identifying risk factors, accessing resources for treatment or support provided on and off campus, and accessing available student accommodations provided on campus;

2. Include a procedure for providing notice of a recommendation for early mental health or substance abuse intervention regarding a student to a parent or guardian of the student within a reasonable amount of time after the identification of early warning signs, which may include declining academic performance, depression, anxiety, isolation, unexplained changes in sleep or eating habits, and destructive behavior toward self and others;

3. Include a procedure for providing notice of a student identified as at risk of committing suicide to a parent or guardian of the student within a reasonable amount of time after the identification of early warning signs;

4. Establish that the School may develop a reporting mechanism and may designate at least one person to act as a liaison officer in the School for the purposes of identifying students in need of early mental health or substance abuse intervention or suicide prevention; and

5. Set out available counseling alternatives for a parent or guardian to consider when his or her child is identified as

possibly being in need of early mental health or substance abuse intervention or suicide prevention.

The practices and procedures must prohibit the use without the prior consent of a student's parent or guardian of a medical screening of the student as part of the process of identifying whether the student is possibly in need of early mental health or substance abuse intervention or suicide prevention.

The practices and procedures developed must be included in the annual student handbook and the School improvement plan under Education Code 11.252. [See BQ]

Nothing in these provisions is intended to interfere with the rights of parents or guardians and the decision-making regarding the best interest of the child. Practices and procedures developed in accordance with these provisions are intended to notify a parent or guardian of a need for mental health or substance abuse intervention so that a parent or guardian may take appropriate action. These provisions do not give Schools the authority to prescribe medications. Any and all medical decisions are to be made by a parent or guardian of a student.

Health and Safety Code 161.325

Immunity

These requirements do not waive any immunity from liability of the School or of school officers or employees, create any liability for a cause of action against the School or against school officers or employees, or waive any immunity from liability under Civil Practice and Remedies Code 74.151. *Health and Safety Code 161.326*

Cybersecurity Policy

The School shall adopt a cybersecurity policy to:

1. Secure school cyberinfrastructure against cyber-attacks and other cybersecurity incidents; and
2. Determine cybersecurity risk and implement mitigation planning.

The School's cybersecurity policy may not conflict with the information security standards for institutions of higher education adopted by the Department of Information Resources (DIR) under Government Code Chapters 2054 and 2059.

Note: In addition to this policy, TSD has adopted a comprehensive set of Information Security Guidelines consistent with the requirements of the Department of Information Resources. These guidelines are shared will all TSD staff on an annual basis and must be acknowledged and followed by all TSD staff.

Cybersecurity Coordinator

The superintendent shall designate a cybersecurity coordinator to serve as a liaison between the School and the Texas Education Agency (TEA) in cybersecurity matters.

Report to TEA

The School's cybersecurity coordinator shall report to TEA any cyber attack or other cybersecurity incident against the school cyberinfrastructure that constitutes a breach of system security as soon as practicable after the discovery of the attack or incident.

Report to Parent

The School's cybersecurity coordinator shall provide notice to a parent of or person standing in parental relation to a student enrolled in the School of an attack or incident for which a report is required to TEA involving the student's information.

Definitions

For purposes of the School's cybersecurity policy, the following definitions apply:

Breach of System Security

"Breach of system security" means an incident in which student information that is sensitive, protected, or confidential, as provided by state or federal law, is stolen or copied, transmitted, viewed, or used by a person unauthorized to engage in that action.

Cyber Attack

"Cyber attack" means an attempt to damage, disrupt, or gain unauthorized access to a computer, computer network, or computer system.

Cybersecurity

"Cybersecurity" means the measures taken to protect a computer, computer network, or computer system against unauthorized use or access.

Education Code 11.175

Cybersecurity Training

At least once each year, the School shall identify School employees who have access to a School computer system or database and require those employees and board members to complete a cybersecurity training program certified under Government Code 2054.519 (State-certified cybersecurity training programs.)

The board or designee may select the most appropriate state-certified cybersecurity training program or school training program for employees of the school to complete. The board or designee shall:

1. Verify and report on the completion of a cybersecurity training program by school employees to the DIR; and
2. Require periodic audits to ensure compliance with these provisions.

Gov't Code 2054.5191(b)

Security Breach Notification

To Individuals

The School owns, licenses, or maintains computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made without unreasonable delay and in each case not later than the 60th day after the date on which the School determines that the breach occurred, except as provided at Criminal Investigation Exception, below, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Resident of Other State

If the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident of a state that requires a person that owns or licenses computerized data to provide notice of a breach of system security, the notice of the breach of system security required under Notice, below, may be provided under that state's law or under Notice, below.

To the Owner or License Holder

The School maintains computerized data that includes sensitive personal information not owned by the School shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Notice

The School may give the required notice to individuals or the owner or license holder by providing:

1. Written notice at the last known address of the individual;
2. Electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001 (electronic records and signatures); or
3. If the School demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the School does not have sufficient contact information, by:
    a. Electronic mail, if the School has electronic mail addresses for the affected persons;
    b. Conspicuous posting of the notice on the School website; or
    c. Notice published in or broadcast on major statewide media.

Information Security Policy

The School maintains its own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice described above complies with the notice requirements if the School notifies affected persons in accordance with that policy.

To the Attorney General

The School is required to disclose or provide notification of a breach of system security under these provisions shall notify the attorney general of that breach not later than the 60th day after the date on which the School determines that the breach occurred if the breach involves at least 250 residents of this state. The notification must include:

1. A detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach;
2. The number of residents of this state affected by the breach at the time of notification;
3. The measures taken by the School regarding the breach;
4. Any measures the School intends to take regarding the breach after the notification described at Notice, above; and
5. Information regarding whether law enforcement is engaged in investigating the breach.

To a Consumer Reporting Agency

If the School is required to notify at one time more than 10,000 persons of a breach of system security, the School shall also notify each consumer reporting agency, as defined by 15 U.S.C. 1681a, that maintains files on consumers on a nationwide basis, of the

timing, distribution, and content of the notices. The School shall provide the notice without unreasonable delay.

Criminal Investigation Exception

The School may delay providing the required notice to individuals or the owner or license holder at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation.

Business and Commerce Code 521.053; Local Gov't Code 205.010

Definitions

For purposes of security breach notifications, the following definitions apply:

Breach of System Security

"Breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner. *Business and Commerce Code 521.053(a)*

Sensitive Personal Information

"Sensitive personal information" means:

1. An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
    a. Social security number;
    b. Driver's license number or government-issued identification number; or
    c. Account number or 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; or
2. Information that identifies an individual and relates to:
    a. The physical or mental health or condition of the individual;
    b. The provision of health care to the individual; or
    c. Payment for the provision of health-care to the individual.

"Sensitive personal information" does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.

Business and Commerce Code 521.002(a)(2), (b)

Cybersecurity Information Sharing Act

The School may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-federal entity or the federal government a cyber threat indicator or defensive measure in accordance with the Cybersecurity Information Sharing Act, 6 U.S.C. Subchapter I (sections 1501–1510). *6 U.S.C. 1503(c)*

Removal of Personal Information

The School sharing a cyber threat indicator pursuant to these provisions shall, prior to sharing:

1. Review such indicator to assess whether it contains any information not directly related to a cybersecurity threat that the School knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information; or

2. Implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the School knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.

6 U.S.C. 1503(d)(2)

Definitions

For purposes of the Cybersecurity Information Sharing Act, the following definitions apply:

Cybersecurity Purpose

"Cybersecurity purpose" means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability. *6 U.S.C. 1501(4)*

Cybersecurity Threat

"Cybersecurity threat" means an action, not protected by the First Amendment to the United States Constitution, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. The term does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement. *6 U.S.C. 1501(5)*

Cyber Threat Indicator

"Cyber threat indicator" means information that is necessary to describe or identify:

1. Malicious reconnaissance, as defined in 6 U.S.C. 1501(12), including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
2. A method of defeating a security control or exploitation of a security vulnerability;
3. A security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
4. A method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
5. Malicious cyber command and control, as defined in 6 U.S.C. 1501(11);
6. The actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
7. Any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
8. Any combination thereof.

6 U.S.C. 1501(6)

Defensive Measure

"Defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability. The term does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by the private entity operating the measure or another entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure. *6 U.S.C. 1501(7)*

Information System

"Information system" has the meaning given the term in 44 U.S.C. 3502 and includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers. *6 U.S.C. 1501(9)*

Security Control "Security control" means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information. *6 U.S.C. 1501(16)*

Security Vulnerability "Security vulnerability" means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control. *6 U.S.C. 1501(17)*

Access to Electronic Communications

Electronic Communication Privacy Act

Except as otherwise provided in the Electronic Communication Privacy Act, 18 U.S.C. 2510–22, a person commits an offense if the person:

1. Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication;

2. Intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:

    a. Such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

    b. Such device transmits communications by radio, or interferes with the transmission of such communication; or

    c. Such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

    d. Such use or endeavor to use takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

    e. Such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

3. Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the

information was obtained through the prohibited interception of a wire, oral, or electronic communication;

4. Intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the prohibited interception of a wire, oral, or electronic communication; or

5. Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by 18 U.S.C. 2511(2)(a)(ii), 2511(2)(b)–(c), 2511(2)(e), 2516, and 2518; knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation; having obtained or received the information in connection with a criminal investigation; and with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation.

It shall not be unlawful for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any state.

18 U.S.C. 2511(1), (2)(d)

Stored Wire and Electronic Communications and Transactional Records Access Act

The School must comply with the Stored Wire and Electronic Communications and Transactional Records Access Act, 18 U.S.C. 2701–12.

Whoever intentionally accesses without authorization a facility through which an electronic communication service is provided or intentionally exceeds an authorization to access that facility and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system commits an offense. *18 U.S.C. 2701(a)*

Exceptions

This section does not apply with respect to conduct authorized:

1. By the person or entity providing a wire or electronic communications service;

2. By a user of that service with respect to a communication of or intended for that user; or

3. By sections 18 U.S.C. 2703, 2704, or 2518.

18 U.S.C. 2701(c)

Definitions

Electronic Communication

"Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce. *18 U.S.C. 2510(12), 2711(1)*

Electronic Storage

"Electronic storage" means:

1. Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

2. Any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

18 U.S.C. 2510(17), 2711(1)

The term encompasses only the information that has been stored by an electronic communication service provider. Information that an individual stores to the individual's hard drive or cell phone is not in electronic storage under the statute. *Garcia v. City of Laredo, 702 F.3d 788 (5th Cir. 2012)*

Electronic Communications System

"Electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. *18 U.S.C. 2510(14), 2711(1)*

Electronic Communication Service

"Electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications. *18 U.S.C. 2510(15), 2711(1)*

Facility

"Facility" includes servers operated by electronic communication service providers for the purpose of storing and maintaining electronic storage. The term does not include technology, such as cell phones and computers, that enables the use of an electronic communication service. *Garcia v. City of Laredo, 702 F.3d 788 (5th Cir. 2012)*

Person

"Person" means any employee, or agent of the United States or any state or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation. *18 U.S.C. 2510(6), 2711(1)*