SEC. 4.28.1. INTRODUCTION

It is the policy of Erath Excels Academy to:

(a) Prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;
(b) Prevent unauthorized access and other unlawful online activity;
(c) Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
(d) Comply with the Children's Internet Protection Act ("CIPA"), the Neighborhood Children's Internet Protection Act ("NCIPA"), and the Protecting Children in the 21st Century Act, to the extent such laws are applicable to Erath Excels Academy.[1]
(e) Establish a cybersecurity program and comply with applicable law regarding cybersecurity breach notifications and data breach notifications, to the extent such laws are applicable to Erath Excels Academy.

It is the goal of this policy not only to prevent and protect, but also to educate employees, students, parents and the Erath Excels Academy community in Internet safety. The CIPA guidelines for an Internet Safety Policy have also been incorporated by Erath Excels Academy into its Acceptable Use Policy and/or Acceptable Use Agreement(s). All limitations and penalties set forth in the Acceptable Use Policy and/or Acceptable Use Agreement(s) are deemed to be incorporated into this policy. Terms used in this policy and that also appear in CIPA have the meanings defined in CIPA.

SEC. 4.28.3. INTERNET SAFETY, COMPLIANCE WITH THE REQUIREMENTS OF CIPA

Sec. 4.28.3.1. Technology Protection Measures

A Technology Protection Measure is a specific technology that blocks or filters Internet access.[2] It must protect against access by adults and minors to visual depictions that are obscene, involve child pornography, or are harmful to minors. Erath Excels Academy utilizes a sophisticated content filtering system that is compliant with CIPA and NCIPA on all computers that access the Internet.

---

[1] CIPA requires recipients of federal technology funds to comply with certain Internet filtering and policy requirements. Schools and libraries receiving funds for Internet access and/or internal connection services must also meet the Internet safety policies of the NCIPA that addresses the broader issues of electronic messaging, disclosure of personal information of minors, and unlawful online activities. The Protecting Children in the 21st Century Act adds an additional Internet Safety Policy requirement covering the education of minors about appropriate online behavior.

[2] As defined by CIPA, the term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

1. Obscene, as that term is defined in section 1460 of title 18, United States Code;
2. Child Pornography, as that term is defined in section 2256 of title 18, United States Code; or
3. Harmful to minors.

Sec. 4.28.3.1. Access to Inappropriate Material

To the extent practical, Technology Protection Measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communication, access to inappropriate information. Specifically, as required by CIPA, blocking shall be applied to visual and textual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to administrative approval, technology protection measures may be disabled or, in the case of minors, minimalized only for bona fide research or other lawful purposes.

Any attempt to bypass, defeat, or circumvent the Technology Prevention Measures is punishable as a violation of this policy and of the Acceptable Use Policies.

Sec. 4.28.3.1. Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of Erath Excels Academy's online computer network when using electronic mail, chat rooms, blogging, instant messaging, online discussions and other forms of direct electronic communications. Without limiting the foregoing, access to such means of communications is strictly limited by the Acceptable Use Policies.

Specifically, as required by CIPA, prevention of inappropriate network usage includes:

(1) unauthorized access, including so-called "hacking" and other unlawful activities; and
(2) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Sec. 4.28.3.1. Supervision and Monitoring

It shall be the responsibility of all professional employees (pedagogical and administrative staff) to supervise and monitor usage of Erath Excels Academy's computers, computer network and access to the Internet in accordance with this policy, the Acceptable Use Policies, and CIPA. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of each Principal or designee.

The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2256 of title 18, United States Code.

Sec. 4.28.3.1. Education

Erath Excels Academy will advocate and educate employees, students, parents and Erath Excels Academy community on Internet safety and "cyber-bullying." Education will be provided through such means as professional development training and materials to employees, Parental Engagement presentations and the Erath Excels Academy website.

Additionally, the Principal or designee will provide age-appropriate training for students who use Erath Excels Academy's Internet facilities. The training provided will be designed to promote Erath Excels Academy's commitment to:

(1) The standards and acceptable use of Internet services set forth in the Acceptable Use Policies.
(2) Student safety with regard to:
    a. safety on the Internet;
    b. appropriate behavior while online, on social networking Web sites, and in chat rooms; and
    c. cyber-bullying awareness and response.
(3) Compliance with the E-rate requirements of CIPA.

Following receipt of this training, the student will acknowledge that he/she has received the training, understood it, and will follow the provisions of the Acceptable Use Policy and/or Acceptable Use Agreement(s).

Sec. 4.28.3.1. Cyberbullying

The Acceptable Use Policies include provisions intended to prohibit and establish penalties for inappropriate and oppressive conduct, including cyber-bullying.

Erath Excels Academy is a place of tolerance and good manners. Students may not use the network or any Erath Excels Academy computer facilities for hate mail, defamatory statements, statements intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion, national origin, gender, sexual orientation or disability.

Network users may not use vulgar, derogatory, or obscene language. Network users also may not post inappropriate anonymous messages or forge e-mail or other messages.

Furthermore, Erath Excels Academy computers and network facilities may not be used for any activity, or to transmit any material, that violates United States, State of Texas, or local laws. This includes, but is not limited to, any threat or act of intimidation or harassment against another person.

Sec. 4.28.4.1. CYBERSECURITY

Sec. 4.28.4.1. Cybersecurity Policy

Erath Excels Academy shall adopt a cybersecurity policy[3] to:

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

Sec. 4.28.4.1. 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 and as required by law report to TEA breaches of system security.[4]

Sec. 4.28.4.1. Report to TEA

Erath Excels Academy's cybersecurity coordinator shall report to TEA, or, if applicable, the entity that administers a system developed by the TEA and the Texas Department of Information Resource (DIR) to coordinate the anonymous sharing of information concerning cyber-attacks or other cybersecurity incidents between schools and the state, 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.[5]

Sec. 4.28.4.1. 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.[6]

[3] A cybersecurity policy is not required by law for open-enrollment charter schools, but is recommended as best practice. A sample Information Security Policy Template is provided Texas Gateway for online resources. This template originated from Texas Gateway and has been slightly revised to address open-enrollment charter schools. It contains suggested policy templates. Additional resources concerning cybersecurity can be found at texasgateway.org/resource/cybersecurity-tools-and-resources.

[4] A designed cybersecurity coordinator is not required by law for open-enrollment charter schools, but is recommended as best practice.
[5] Texas Education Code §11.175(e).
[6] Texas Education Code §11.175(f).

Sec. 4.28.4.1. Definitions

For purposes of this section, the following definitions apply:

"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.[7]

"Cyber-attack" means an attempt to damage, disrupt, or gain unauthorized access to a computer, computer network, or computer system.[8]

"Cybersecurity" means the measures taken to protect a computer, computer network, or computer system against unauthorized use or access.[9]

Sec. 4.28.4.1. Cybersecurity Training

Each Erath Excels Academy employee and Board member shall annually complete a cybersecurity training program designated by Erath Excels Academy. Additionally, Erath Excels Academy shall complete periodic audits to ensure compliance with the cybersecurity training requirements.[10]

Sec. 4.28.4.1. SECURITY BREACH NOTIFICATION

Sec. 4.28.4.1. To Individuals

A School that 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.[11]

---

[7] Texas Education Code §11.175(a).
[8] Texas Education Code §11.175(a).
[9] Texas Education Code §11.175(a).
[10] This is not required by law for open-enrollment charter schools, but is recommended as best practice. Texas Gateway provides information on cybersecurity training programs and free cybersecurity training through Cybrary: https://www.texasgateway.org/resource/cybersecurity-tips-and-tools
[11] Tex. Bus. & Com. §521.053(b).

Sec. 4.28.4.1. 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.[12]

Sec. 4.28.4.1. To the Owner or License Holder

A School that 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.[13]

Sec. 4.28.4.1. Notice

Upon discovering or receiving notification of a breach of system security, Erath Excels Academy shall disclose the breach to affected persons or entities in accordance with the time frames established by law and this policy.

Sec. 4.28.4. Erath Excels Academy shall give notice by using one or more of the following methods in compliance with applicable law[14]:

(1) Written notice.

(2) Electronic mail, if Erath Excels Academy has electronic mail addresses for the affected persons.

(3) Conspicuous posting on Erath Excels Academy's website.

(4) Publication through broadcast media.

Sec. 4.28.4.1. Information Security Policy

A School that 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.

[12] Tex. Bus. & Com. §521.053(b-1).
[13] Tex. Bus. & Com. §521.053(c).
[14] Tex. Bus. & Com. §521.053(e), (f).
[15] Tex. Bus. & Com. §521.053(g).

Sec. 4.28.4.1. To the Attorney General[16]

A school that 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 number of affected residents that have been sent a disclosure of the breach by mail or other direct method of communication at the time of notification;
(4) The measures taken by the School regarding the breach;
(5) Any measures the School intends to take regarding the breach after the notification described at Notice, above; and
(6) Information regarding whether law enforcement is engaged in investigating the breach.

Sec. 4.28.4.1. 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.[17]

Sec. 4.28.4.1. Criminal Investigation Exception

A 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.[18]

---

[16] Tex. Bus. & Com. §521.053(i).
[17] Tex. Bus. & Com. §521.053(h).
[18] Tex. Bus. & Com. §521.053(d).

Sec. 4.28.4.1. Definitions

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

"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.[19]

"Sensitive personal information"[20] 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.

[19] Tex. Bus. & Com. §521.053(a).
[20] Tex. Bus. & Com. §521.053(a)(2),(b).