Technology Policies
Table of Contents

T-1 FERPA - Student Scholastic Record Management

Resource(s):

- 53A-13-301 Utah Family Educational Rights and Privacy Act
- 20 U.S.C §1232(g) Family Educational Rights and Privacy Act, 34 CFR Part 99
- 20 U.S.C §1232(h) Protection of Pupil Rights Amendment, 34 CFR Part 98
- R277-487 Family and Student Records

I. General Procedures

A. All information regarding students and their families shall be collected and maintained under safeguards of privacy established by federal and state laws or regulations.

B. An accurate and complete individual, permanent and cumulative record shall be maintained for each student enrolled at East Hollywood High School.

1. When appropriate, a separate confidential record shall be maintained for those students requiring differentiated programs and/or special services such as gifted and talented and students with special needs.
2. When a separate confidential record is established a notation on the cumulative record shall indicate the location of the confidential records. All data (cumulative and confidential) shall be considered the student's official scholastic records.

C. All personnel authorized access to scholastic records shall be informed of this policy and it's implementing regulations.

D. The employee responsible for the in-service education of records maintenance personnel and the collection, security, use, disclosure, periodic evaluation, transfer and destruction of scholastic records data shall be designated as custodian of student records.

E. The custodian of student records at EHHS shall be the principal or a designee. The Director of Special Education at EHHS shall maintain or designate a custodian to maintain the confidential Individual Education Program (IEP) file.

F. All documents in the student cumulative/permanent record file, which include directory information, ethnic origin, schools and years attended, subjects completed, grades and credits earned, competency evaluations, certain health records, and other documents related to the education program, are private records with the exception of certain directory information.

G. Student records shall be accessible to:

1. Authorized school personnel having responsibility for the student's educational program, and to individuals conducting federal, state, or district audits of educational programs.
   a) Parents.
      (1) In the event that parents are divorced or separated, both parents shall be entitled to access their child's student records unless prohibited by court order.
      (2) Eligible students.

H. Except in accordance with state and federal law, access to student records shall not be given to individuals other than those listed is Section (G) above.

I. Certain student information designated as "directory information" may be made public without prior written consent. However, there is no legal requirement that a school

release directory information about a student. EHHS has designated the following student information as directory information:

1. Student's name, address, and telephone listing
2. Participation in officially recognized activities and sports
3. Weight and height of members of athletic teams
4. Dates of enrollment at a school
5. Degrees and awards received
6. The most recent or previous educational agency or institution attended by the student
7. Current grade in school and teacher(s)
8. Yearbook photos

J. Parents or students who do not want this information to be made public will be given an opportunity each year to notify the school that such information is not to be made public through the Annual Notice.

K. A copy of the Annual Notice, which includes information on access rights, must be included in student registration packets and all student handbooks, posted on the school website, and otherwise widely distributed and made available to parents.

L. The Student Information Military and College Recruiting Opt-Out Form must also be included in high school registration packets, published in high school handbooks, posted on the school website, and otherwise widely distributed and made available to parents.

II. Requests to Review Student Records

A. Parents of students currently enrolled or eligible students may submit a written request to the school principal or designee to review or obtain copies of their student's record.

B. Before allowing a person access to student records, school personnel must verify the identity of the person making the request.

C. Directory information should not routinely be released to the public or media. School employees should contact the Utah State Office – Records Department if they have questions about requests they may receive. Access to school records under the Family Educational Rights and Privacy Act (FERPA) pertains only to official educational records, such as grades, attendance, and other information found in the cumulative file. It does not extend to classroom records held by an individual teacher, principal, counselor, or other staff.

D. Schools are not required to prepare special reports or to recreate lost or destroyed records to satisfy a request for student records.

E. Copies of records must be provided to parents and eligible students at a reasonable cost. Inability to pay reproduction costs may not prohibit access to the record itself.

F. Requests for access to records should be granted in a timely manner; however, schools have up to 45 days to reply to a request.

G. Except for those individuals listed below, schools must maintain a record of each request for access to, and each disclosure they make from, an education record.

1. The record of access must include the names of parties who have requested or received information from the records, and the stated reason for the request.
2. A copy of the signed parent consent to release a record must be kept in the student's cumulative file.

H. Schools are not required to keep a log or other record of access if the request is from, or the disclosure made to, any of the following:
   1. The parent or eligible student
   2. A properly designated school official for a legitimate educational purpose
   3. A party seeking directory information

III. Denial of Release of Student Information

A. When a school receives either a parent's or eligible student's written authorization to deny the release of their student's directory information, or a signed Military and College Recruiting Opt-Out Form, the school will document that authorization in the student information system in a timely manner and in such a way that any employee may readily determine whether to deny disclosure of the student's directory information.
B. When a parent or eligible student chooses the option of denying the release of their student's directory information, they are opting out of the release of all directory information. Parents may not select items or circumstances under which some information may or may not be released.
C. Once an eligible student or parent has made a request to deny the release of the student's directory information, the request will be effective in successive school years, unless changed in writing by the eligible student or parent.
D. Schools must monitor each request to deny the release of a student's directory information to ensure that the request is honored.
E. At the senior high school level, all requests for student names, addresses, and telephone listings received from military recruiters or institutions of higher education will be referred to the district's director of information systems and technology for a response.
F. Before releasing a student's directory information, the director of information systems and technology or school principal will verify, to the best of his or her ability, whether any documentation restricting the release of such information exists.

IV. Requests to Amend Student Records

A. If a parent or eligible student believes their student's record contains information that is inaccurate, misleading, or in violation of the student's right of privacy, he or she may request that the record be amended or corrected.
B. Parents should submit a written request to the principal seeking a review of their student's record. Parents should cite information they believe to be inaccurate, misleading, or a violation of their child's privacy rights and provide any documentation that supports their belief.
C. The principal will review the record, gather more information, and may conference with the parents to clarify their concerns.
D. The principal will render a decision within 20 school days of the receipt of the request.
E. If a parent wishes to appeal the principal's decision, he or she may send a written request for a hearing to the school's director within ten school days of the principal's decision.
F. The director will refer the appeal to the president of the Board of Trustees, who will conduct a hearing within 20 school days.
G. Parents will have the opportunity to present evidence supporting their request that the record be changed.

H. Parents may be assisted or represented by one or more individuals, including their attorney; however, parents must give advanced notice if they intend to bring legal counsel, so that the district also has the opportunity to have legal representation present at the hearing.

I. The Board of Trustees will render a written decision within 20 school days. The decision will include a summary of the evidence and the basis for the decision.

J. If the decision is made to amend or correct the student's record, the amendment will be made and the parent will be informed of the amendment in writing.

K. If the Board of Trustees determines that the record will not be changed, the parent may place a statement in the student's record commenting on the contested information and/or an explanation of why he or she disagrees with the Governing Boards decision.

V. Requests for Records by Subpoena or in an Emergency

A. Before releasing student information pursuant to a subpoena, the school should notify the parent that their child's records have been subpoenaed so that the parent has the opportunity to seek legal counsel, and seek to quash the subpoena.

B. School officials may disclose student information to appropriate parties in an emergency situation if the sharing of the information is necessary to protect the health or safety of an individual.

C. Prior Written Notification and Consent Required for Student Participation in Certain Activities Prior written consent from parents or guardians must be obtained before students are asked to complete written assignments, answer questions, complete questionnaires, or take psychological or psychiatric examinations, tests, or treatments which reveal any of the following information about the student or the student's family, whether such information is personally identifiable or not:

1. Political affiliations; except as provided for in state law, political philosophies
1. Mental or psychological problems Sexual behavior, orientation, or attitudes
2. Illegal, anti-social, self-incriminating, or demeaning behavior
3. Critical appraisal of individuals with whom the student or family member has close family relationships
4. Religious affiliations or beliefs
5. Legally recognized privileged and analogous relationships, such as those with lawyers, medical personnel, or ministers
6. Income, except as required by law

D. Prior written consent under Section (A) above is required in all grades, kindergarten through grade twelve. The prohibitions included in Section (A) also apply within the curriculum and other school activities unless appropriate prior written consent has been obtained.

E. In order for the prior written consent to be valid, parents or guardians must be given notification at least two weeks before any information outlined in Section (A) is solicited.

F. This notice must include information that a copy of the educational or student survey questions to be asked is available at the school for the parents to review.

G. This notice must provide parents a reasonable opportunity to obtain written information concerning:

1. Records or information, including information about relationships, that may be examined or requested
2. The means by which the records or information shall be examined or reviewed

3. The means by which the information is to be obtained
4. The purposes for which the records or information are needed
5. The entities or persons, regardless of affiliation, who will have access to the personally identifiable information
6. A method by which a parent can grant permission to access or examine the personally identifiable information

H. School staff will provide appropriate consent forms to parents and will monitor student participation as per written parental consent.

I. Unless otherwise agreed to by the parent and the person requesting written consent, the authorization is valid only for the activity for which it was granted.

J. Following disclosure, parents may waive the two week minimum notification period.

K. The two week prior written notification requirement is not applicable in a situation which a school employee reasonably believes to be an emergency, in relation to child abuse or neglect reports, or by order of the court.

L. This policy does not limit the ability of a student to spontaneously express sentiments or opinions otherwise protected from disclosure.

M. If a school employee or agent believes that a situation exists which presents a serious threat to the well-being of a student, that employee or agent shall notify the student's parent without delay. If, however, the matter has been reported to the Division of

N. Child and Family Services (DCFS), it is the responsibility of DCFS to notify the student's parent. (See, Child Abuse).

O. These procedures outlining the need for prior written notification and consent in certain circumstances, are necessary in order for the district to comply with the Utah Family Educational Rights and Privacy Act (UFERPA) and the Protection of Pupil Rights Amendment (PPRA). (See, UFERPA at Utah Code Ann. §53A-13-302, and PPRA at 20 U.S.C. §1232(h); 34 C.F.R. Part 98.)

P. School employees violating these procedures may be subject to discipline, up to and including termination.

VI. Media Requests and Internet Safety

A. Unless the release of a student's information has been prohibited (see, Section III), a student may be photographed or videotaped by news media during coverage of school events or programs.

B. In accordance with the Children's Internet Protection Act (CIPA), the EHHS has developed an Internet safety plan that protects students from the unauthorized disclosure, use, and dissemination of their personal information on the Internet.

VII. Notification of Student Data Breach

A. EHHS must notify the parent of a student if there is a release of the student's personally identifiable student data due to a security breach.

T-2 Technology Security Policy

Resource(s)

- 20 U.S. Code §1232g Family Rights and Privacy Act
- U.C.A. §62G-2 Government Records and Management Act
- U.C.A. §53A-1-1401 Student Data Protection Act
- 15 U.S. Code §§ 6501–6506 Children's Online Privacy Protection Rule
- Utah Administrative Code R277-487 Student Data Protection Act

I. Purpose

A. The purpose of this policy is to ensure the secure use and handling of all EHHS data, computer systems and computer equipment by EHHS students, patrons, and employees.

II. Policy

A. Technology Security

1. It is the policy of EHHS to support secure network systems at EHHS, including security for all personally identifiable information that is stored on paper or stored digitally on EHHS-maintained computers and networks. This policy supports efforts to mitigate threats that may cause harm to EHHS, its students, or its employees.
2. EHHS will ensure reasonable efforts will be made to maintain network security. Data loss can be caused by human error, hardware malfunction, natural disaster, security breach, etc., and may not be preventable.
3. All persons who are granted access to the EHHS network and other technology resources are expected to be careful and aware of suspicious communications and unauthorized use of EHHS devices and the EHHS network. When an employee or other user becomes aware of suspicious activity, (s)he is to immediately contact the EHHS's Information Security Officer with the relevant information.
4. This policy and procedure also covers third party vendors/contractors that contain or have access to EHHS critically sensitive data. All third party entities will be required to sign the *Restriction on Use of Confidential Information Agreement* before accessing our systems or receiving information. It is the policy of EHHS to fully conform with all federal and state privacy and data governance laws. Including the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (hereinafter "FERPA"), the Government Records and Management Act U.C.A.§62G-2 (hereinafter "GRAMA"), U.C.A. §53A-1-1401 et seq and Utah Administrative Code R277-487.
5. Professional development for staff and students regarding the importance of network security and best practices are included in the procedures. The procedures associated with this policy are consistent with guidelines provided by cyber security professionals worldwide and in accordance with Utah Education Network and the

Utah State Office of Education. EHHS supports the development, implementation and ongoing improvements for a robust security system of hardware and software that is designed to protect EHHS's data, users, and electronic assets.

III. Definitions:

A. **Access:** Directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them.
B. **Authorization:** Having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.
C. **Computer:** Any electronic device or communication facility that stores, retrieves, processes, or transmits data.
D. **Computer system:** A set of related, connected or unconnected, devices, software, or other related computer equipment. Computer network: The interconnection of communication or telecommunication lines between: computers; or computers and remote terminals; or the interconnection by wireless technology between: computers; or computers and remote terminals.
E. **Computer property:** Includes electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them.
F. **Confidential:** Data, text, or computer property that is protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission.
G. **Encryption or encrypted data:** The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.
H. **Personally Identifiable Information (PII):** Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered protected data.
I. **Security system:** A computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption, password protection, other forced authentication, or access control designed to keep out unauthorized persons.
J. **Sensitive data:** Data that contains personally identifiable information.
K. **System level:** Access to the system that is considered full administrative access. Includes operating system access and hosted application access.

IV. Security Responsibility

A. The EHHS Director of Information Technology shall act as its IT Security Officer (ISO) responsible for overseeing EHHS-wide IT security, to include development of EHHS policies and adherence to the standards defined in this document.

V. Training

A. EHHS, led by the ISO, shall ensure that all EHHS employees having access to sensitive information undergo annual IT security training which emphasizes their personal responsibility for protecting student and employee information. - Training resources will be provided to all EHHS employees.

1. EHHS, led by the ISO, shall ensure that all students are informed of Cyber Security Awareness.

VI. Physical Security

A. Computer Security

1. EHHS shall ensure that any user's computer must not be left unattended and unlocked, especially when logged into sensitive systems or data including student or employee information. Automatic log off, locks and password screen savers should be used to enforce this requirement.
2. EHHS shall ensure that all equipment that contains sensitive information will be secured to deter theft.
3. Server/Network Room Security

a) EHHS shall ensure that server rooms and telecommunication rooms/closets are protected by appropriate access control which segregates and restricts access from general school or EHHS office areas. Access control shall be enforced using either keys, electronic card readers, or similar method with only those IT or other staff members having access necessary to perform their job functions are allowed unescorted access.

(1) Telecommunication rooms/closets may only remain unlocked or unsecured when because of building design it is impossible to do otherwise or due to environmental problems that require the door to be opened.

VII. Contractor access

A. Before any contractor is allowed access to any computer system, server room, or telecommunication room the contractor will need to present a company issued identification card, and his/her access will need to be confirmed directly by the authorized employee who issued the service request or by EHHS's Director of Technology.

VIII. Network Security

A. Network perimeter controls will be implemented to regulate traffic moving between trusted internal (EHHS) resources and external, untrusted (Internet) entities. All network transmission of sensitive data should enforce encryption where technologically feasible.

1. Network Segmentation

a) EHHS shall ensure that all untrusted and public access computer networks are separated from main EHHS computer networks and utilize security policies to ensure the integrity of those computer networks.

b) EHHS will utilize industry standards and current best practices to segment internal computer networks based on the data they contain. This will be done to prevent unauthorized users from accessing services unrelated to their job duties and minimize potential damage from other compromised systems.

2. Wireless Networks
   a) No wireless access point shall be installed on EHHS's computer network that does not conform to current network standards as defined by the Network Manager. Any exceptions to this must be approved directly in writing by the Information Security Officer.
   b) EHHS shall scan for and remove or disable any rogue wireless devices on a regular basis.
   c) All wireless access networks shall conform to current best practices and shall utilize at minimal WPA encryption for any connections. Open access networks are not permitted, except on a temporary basis for events when deemed necessary.
3. Remote Access
   a) EHHS shall ensure that any remote access with connectivity to the EHHS's internal network is achieved using the EHHS's centralized VPN service that is protected by multiple factor authentication systems. Any exception to this policy must be due to a service provider's technical requirements and must be approved by the Information Security Officer.
4. Access Control
   a) System and application access will be granted based upon the least amount of access to data and programs required by the user in accordance with a business need- to-have requirement.
5. Authentication
   a) EHHS shall enforce strong password management for employees, students, and contractors.
   b) Password Creation
      (1) All server system-level passwords must conform to guidelines created by the Information Security Officer.
   c) Password Protection
      (1) Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
      (2) Passwords must not be inserted into email messages or other forms of electronic communication.
      (3) Passwords must not be revealed over the phone to anyone.
      (4) Do not reveal a password on questionnaires or security forms.
      (5) Do not hint at the format of a password (for example, "my family name").
      (6) Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.
6. Authorization
   a) EHHS shall ensure that user access shall be limited to only those specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

b) EHHS shall ensure that user access should be granted and/or terminated upon timely receipt, and management's approval, of a documented access request/termination.

7. Accounting
   a) EHHS shall ensure that audit and log files are maintained for at least ninety days for all critical security-relevant events such as: invalid logon attempts, changes to the security policy/ configuration, and failed attempts to access objects by unauthorized users, etc.
8. Administrative Access Controls
   a) EHHS shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.
9. Incident Management
   a) Monitoring and responding to IT related incidents will be designed to provide early notification of events and rapid response and recovery from internal or external network or system attacks.
10. Business Continuity
   a) To ensure continuous critical IT services, IT will develop a business continuity/disaster recovery plan appropriate for the size and complexity of EHHS IT operations.
   b) EHHS shall develop and deploy a EHHS-wide business continuity plan which should include as a minimum:
      (1) Backup Data: Procedures for performing routine daily/weekly/monthly backups and storing backup media at a secured location other than the server room. As a minimum, backup media must be stored off-site at a reasonably safe distance from the primary server room.
      (2) Secondary Locations: Identify a backup processing location such as another building associated with EHHS.
      (3) Emergency Procedures: Document a calling tree with emergency actions to include: recovery of backup data, restoration of processing at the secondary location, and generation of student and employee listings for ensuing a full head count of all.
11. Malicious Software
   a) Server and workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.
   b) EHHS shall install, distribute, and maintain spyware and virus protection software on all EHHS-owned equipment, i.e. servers, workstations, and laptops.
   c) EHHS shall ensure that malicious software protection will include frequent update downloads (minimum weekly), frequent scanning (minimum weekly), and that malicious software protection is in active state (real time) on all operating servers/workstations.
   d) EHHS shall ensure that all security-relevant software patches (workstations and servers) are applied within thirty days and critical patches shall be applied as soon as possible.

e) EHHS shall ensure that all security-relevant software patches (workstations and servers) are applied within thirty days and critical patches shall be applied as soon as possible.

f) All computers must use EHHS approved anti-virus solution.

g) Any exceptions to section 3.9 must be approved by the Information Security Officer.

12. Internet Content Filtering

a) In accordance with Federal and State Law, EHHS shall filter internet traffic for content defined by law that is deemed harmful to minors.

b) EHHS acknowledges that technology based filters are not always effective at eliminating harmful content and due to this, EHHS uses a combination of technological means and supervisory means to protect students from harmful online content.

c) In the event that students take devices home, EHHS will provide a technology based filtering solution for those devices. However, EHHS will rely on parents to provide the supervision necessary to fully protect students from accessing harmful online content.

d) Students shall be supervised when accessing the internet and using EHHS owned devices on school property.

13. Data Privacy

a) EHHS considers the protection of the data it collects on students, employees and their families to be of the utmost importance.

b) EHHS protects student data in compliance with the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 ("FERPA"), the Government Records and Management Act U.C.A. §62G-2 ("GRAMA"), U.C.A. §53A-1-1401 et seq, 15 U.S. Code §§ 6501–6506 ("COPPA") and Utah Administrative Code R277-487 ("Student Data Protection Act").

c) EHHS shall ensure that employee records access shall be limited to only those individuals who have specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

IX. Security Audit and Remediation

A. EHHS's IT Security Officer (IT Director) shall perform routine security and privacy audits in congruence with Data Governance Plan.

B. EHHS' shall develop remediation plans to address identified lapses that conforms with the school's Data Governance Plan.

C. Employee Disciplinary Actions shall be in accordance with applicable laws, regulations and EHHS's policies. Any employee found to be in violation may be subject to disciplinary action up to and including termination of employment.

T-3 Data Breach Policy

Resource(s)

- 20 U.S. Code §1232g — Family Rights and Privacy Act
- U.C.A. §62G-2 — Government Records and Management Act
- U.C.A. §53A-1-1401 — Student Data Protection Act
- 15 U.S. Code §§ 6501–6506 — Children's Online Privacy Protection Rule
- R277-487 — Student Data Protection Act
- 53A-1-1404 — Local student data protection governance
- 53A-1-1405 — Student data ownership -- Notification in case of breach

I. Overview

A. Data breaches are increasingly common occurrences whether caused through human error or malicious intent. East Hollywood High School operations rely on the proper use of Confidential Information and Personally Identifiable Information (PII) on a daily basis. Managing risk and responding in an organized way to Incidents and Breaches is key to operations and required by Utah state law.

II. Purpose

A. EHHS must have a robust and systematic process for responding to reported data security Incidents and Breaches. This policy is designed to standardize the EHHS-wide response to any reported Breach or Incident, and ensure that they are appropriately logged and managed in accordance with best practice guidelines. Standardized processes and procedures help to ensure the EHHS can act responsibly, respond effectively, and protect its information assets to the extent possible.

III. GENERAL INFORMATION

A. This policy applies to all EHHS staff.
B. A “Data Security Incident” or “Incident’ shall mean an accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication or information resources of the EHHS.
    1. Common examples of data security Incidents include, but are not limited to, any of the following:
        a) Successful attempts to gain unauthorized access to a EHHS system or Student or Educator PII regardless of where such information is located
        b) Unwanted disruption or denial of service
        c) The unauthorized use of a EHHS system for the processing or storage of Confidential Information or PII
        d) Changes to EHHS system hardware, firmware, or software characteristics without the EHHS’s knowledge, instruction, or consent
        e) Loss or theft of equipment where Confidential Information or PII is stored
        f) Unforeseen circumstances such as a fire or flood that could lead to the loss or misuse of Confidential Information or PII
        g) Human error involving the loss or mistaken transmission of Confidential Information or PII
        h) Hacking, social engineering, phishing or other subversive attacks where information is obtained by deceitful practice

C. A "Data Security Breach" or "Breach" is any Incident where EHHS cannot put in place controls or take action to reasonably prevent the misuse of Confidential Information or PII. A Breach is also an Incident where data has been misused.
   1. Adopting a standardized and consistent approach to Incident management shall ensure that:
      a) Incidents are reported in a timely manner and can be properly investigated
      b) Incidents are handled by appropriately authorized and skilled personnel
      c) Appropriate levels of management are involved in response management
      d) Incidents are recorded and documented
      e) Organizational impacts are understood and action is taken to prevent further damage
      f) Evidence is gathered, recorded, and maintained in a form that will withstand internal and external scrutiny
      g) External agencies, customers, and data users are informed as required
      h) Incidents are dealt with in a timely manner and normal operations are restored
      i) Incidents are reviewed to identify improvements in policies and procedures

D. Incidents can occur locally, in the cloud, or through third party service providers. Reporting and management of Incidents shall occur similarly. Third party providers shall also be governed by contract terms and liability as defined in their operational agreements.

E. Any contract breach that results in the misuse or unauthorized access to Student PII by a School Service Contract Provider must be handled according to EHHS's Board of Trustees Security Breach Policy as required by C.R.S. 22-16-107(2)(a).

IV. DATA CLASSIFICATIONS

A. Incidents vary in impact and risk depending on a number of mitigating factors including the content and quantity of the data involved. It is critically important that EHHS management respond quickly and identify the data classification of the Incident. This allows staff to respond accordingly in a timely and thorough manner.

B. All reported Incidents shall be classified as below in order to assess risk and approaches to mitigate the situation. Data classification shall refer to the following EHHS data categories:
   1. **Public Data** - Information intended for public and community use or information that can be made public without any negative impact on the EHHS or its customers. Student PII shall never be considered public data unless the data is Directory Information as defined by EHHS policy.
   2. **Confidential/Internal Data** - Information of a more sensitive nature to the business and educational operations of EHHS. This data represents basic intellectual capital, applications, and general knowledge. Access shall be limited to only those people that need to know as part of their role within the EHHS. Employee and Educator PII (with the exception of Social Security Numbers (SSN), financial information, or other critical information) falls within this classification.
   3. **Highly Confidential Data**- Information that, if breached, causes significant damage to EHHS operations, reputation, and/or business continuity. Access to this information should be highly restricted. Student PII falls into this category of data. Employee or Educator Financial Information, Social Security Numbers, and other critical information also fall into this classification.

V. INCIDENT REPORTING

A. The following process shall be followed when responding to a suspected Incident:
   1. Confirmed or suspected Incidents shall be reported promptly to the EHHS's Principal/Director and/or designee. A formal report shall be filed that includes full and accurate details of the Incident including who is reporting the Incident and what classification of data is involved.
   2. Once an Incident is reported, EHHS's principal and/or designee shall conduct an assessment to establish the severity of the Incident, next steps in response, and potential remedies and solutions. Based on this assessment, EHHS's principal and/or designee shall determine if this Incident remains an Incident or if it needs to be categorized as a Breach.
   3. All Incidents and Breaches will be centrally logged and documented to ensure appropriate documentation, oversight, and consistency in response, management, and reporting.

VI. CLASSIFICATION

A. Data Breaches or Incidents shall be classified as follows:
   1. **Critical/Major Breach or Incident** – Incidents or Breaches in this category deal with Confidential Information or PII and are on a large scale. All Incidents or Breaches involving Student PII will be classified as Critical or Major. They typically have the following attributes:
      a) Any Incident that has been determined to be a Breach
      b) Significant Confidential Information or PII loss, potential for lack of business continuity, EHHS exposure, or irreversible consequences are imminent
      c) Negative media coverage is likely and exposure is high
      d) Legal or contractual remedies may be required
      e) Requires significant reporting beyond normal operating procedures
      f) Any breach of contract that involves the misuse or unauthorized access to Student PII by a School Service Contract Provider
   2. **Moderately Critical/Serious Incident** – Breaches or Incidents in this category typically deal with Confidential Information and are on a medium scale. Incidents in this category typically have the following attributes:
      a) Risk to the EHHS is moderate
      b) Third party service provider and subcontractors may be involved
      c) Data loss is possible but localized/compartmentalized, potential for limited business continuity losses, and minimized EHHS exposure
      d) Significant user inconvenience is likely
      e) Service outages are likely while the breach is addressed
      f) Negative media coverage is possible but exposure is limited
      g) Disclosure of Educator or Employee PII is contained and manageable
   3. **Low Criticality/Minor Incident** – Incidents in this category typically deal with personal or internal data and are on a small or individualized scale personal or mobile device related). Incidents in this category typically have the following attributes:
      a) Risk to the EHHS is low
      b) User inconvenience is likely but not EHHS damaging
      c) Internal data released but data is not student, employee, or confidential in nature
      d) Loss of data is totally contained on encrypted hardware
      e) Incident can be addressed through normal support channels

VII. INCIDENT RESPONSE

A. Management response to any reported Incident shall involve the following activities:

1. Assess, Contain and Recover Data - All security Incidents shall have immediate analysis of the Incident and an Incident report completed by EHHS's Principal or their designee. This analysis shall include a determination of whether this Incident should be characterized as a Breach. This analysis shall be documented and shared with the [Incident Appropriate Role], the affected parties, and any other relevant stakeholders. At a minimum, the [Insert Appropriate Role] shall:

Step	Action	Notes
A	Containment and Recovery:	Contain the breach, limit further organizational damage, seek to recover/restore data.
1	Breach Determination	Determine if the Incident needs to be classified as a Breach.
2	Ascertain the severity of the Incident or Breach and determine the level of data involved.	See Incident Classification
3	Investigate the Breach or Incident and forward a copy of the Incident report to the Board of Trustees	Ensure investigator has appropriate resources including sufficient time and authority. In the event that the Incident or Breach is severe.
4	Identify the cause of the Incident or breach and whether the situation has been contained. Ensure that any possibility of further data loss is removed or mitigated as far as possible. If this loss cannot be mitigated, any Incident will be characterized as a Breach.	Compartmentalize and eliminate exposure. Establish what steps can or need to be taken to contain the threat from further data loss. Contact all relevant departments who may be able to assist in this process. This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the Incident.
5	Determine depth and breadth of losses and limit exposure/damages	Can data be physically recovered if damaged through use of backups, restoration or other means?
6	Notify authorities as appropriate	For criminal activities where property was stolen or fraudulent activity occurred, contact the appropriate authorities and general counsel. Should the Breach involve Student PII that involves a School Service Contract Provider, notify the EHHS Board members.
7	Ensure all actions and decisions are logged and recorded as part of incident documentation and reporting.	Complete Incident Report and file will be keep on file in the EHHS's Principals office.

B. Assess Risk and Incident Scope – All Incidents or Breaches shall have a risk and scope analysis completed by the EHHS's Principal and IT Director or their designee. This analysis shall be documented and shared with the affected parties, and any other relevant stakeholders. At a minimum, EHHS's Principal and IT Director shall:

B	Risk Assessment	Identify and assess ongoing risks that may be associated with the Incident or Breach.
1	Determine the type and breadth of the Incident or Breach	Classify Incident or Breach type, data compromised, and extent of breach
2	Review data sensitivity	Determine the confidentiality, scope and extent of the Incident or Breach.
3	Understand the current status of the compromised data	If data has been stolen, could it be used for purposes that harm the individuals whose identity has been compromised; If identity theft is involved, this poses a different type and level of risk.
4	Document risk limiting processes or technology components that contain and manage the Incident	Does encryption of data/device help to limit risk of exposure?
5	Determine what technologies or processes will mitigate the loss and restore service	Are there backups of the compromised data? Can they be restored to a ready state?
6	Identify and document the scope, number of users affected, and depth of Incident or Breach	How many individuals' personally identifiable information were affected?
7	Define individuals and roles whose data was compromised	Identify all students, staff, districts, customers or vendors involved in the Incident or Breach
8	If exploited, what will the compromised data tell a third party about the individual? Could it be misused?	Confidential Information or PII could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a criminal build up a detailed picture associated with identity theft or fraud.
9	Determine actual or potential harm that could come to any individuals	Identify risks to individuals: • Physical Safety • Emotional Wellbeing • Personal or Business Reputation • Financial Implications • Identity Concerns
10	Are there wider consequences to consider?	Is there risk to the state, or loss of public confidence?
11	Are there others who might provide support or advise on risks/courses of action?	Contact all local education providers, agencies, or companies impacted by the breached data, notify them about the Incident, and ask for assistance in limiting the scope of the Incident.

C. Notification and Incident Communications - Each security Incident or Breach determined to be “moderately critical” or “critical” shall have communication plans documented by the [Insert Appropriate Role or Roles] senior leadership, and their designees to appropriately manage the Incident and communicate progress on its resolution to all effected stakeholders. At a minimum, the [Insert Appropriate Role] shall:

C	Notification and Communications	Notification enables affected stakeholders to take precautionary steps and allow regulatory bodies to act on the Incident or Breach.
1	Are there legal, contractual or regulatory notification requirements associated with the Incident or Breach?	Review vendor contracts and compliance terms, assure state and federal reporting and notifications are understood. Contact EHHS’s Board of Trustees as necessary to begin contractual adherence. Should the Breach include Student PII, initiate the EHHS Board hearing process.
2	Notify impacted individuals of Incident or Breach remedies.	Provide individuals involved in the Incident or Breach with mitigation strategies to re-secure data (e.g. change user id and/or passwords etc.)
3	Determine Internal Communication Plans	Work with senior leadership and provide regular internal updates on status of Incident or Breach, remedies underway, and current exposure and containment strategies. This messaging should be provided to all internal state stakeholders and management. Messaging shall be coordinated through the [Insert Appropriate Department] office.
4	Determine Public Messaging	Prepare and execute a communication and follow-up plan with EHHS’s Data Advisory Group. Communication strategies need to define audience(s), frequency, messaging, and content.

5	Execute Messaging Plan	Working through EHHS's Data Governance Plan and Data Advisory Group, execute the public and internal communication plans. Depending on the nature and scope of the Incident or Breach, multiple messages may need to be delivered as well as press and public communiques. Minimally notifications should include: • A description of the Incident or Breach (how and when it occurred) • What data was involved and whose data was compromised • Details of what has been done to respond to the Incident or Breach and any associated risks posed • Next-steps for stakeholders • EHHS contacts for the Incident or Breach • When notifying individuals, provide specific and clear advice on the steps they can take to protect themselves and what the EHHS and/or third party vendor will do to help minimize their exposure • Provide a way in which they can contact EHHS for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or a web page)

D. Post Mortem Evaluation and Response – Each Incident or Breach determined to be "moderately critical" or "critical" shall have a post mortem analysis completed by the EHHS's IT Director, Principal and/or their designees to appropriately document, analyze, and make recommendations on ways to limit risk and exposure in the future. At a minimum, EHHS's Principal and IT Director shall:

D	Evaluation and Response	To evaluate the effectiveness of the University's response to the Incident or Breach.
1	Establish where any present or future risks lie.	Assess and evaluate the root causes of the Incident or Breach and any ways to mitigate and/or prevent a similar occurrence.
2	Consider the data and security measures employed.	Evaluate, analyze, and document the use cases and technical components of the Incident or Breach. Document areas for improvement in environment, technology, or approach that limit future security exposures. Make recommendations as appropriate.
3	Evaluate and identify areas of weakness in existing security measures and procedures.	Document lapses in process, procedure, or policy that may have caused the Incident or Breach. Analyze and document solutions and remedies to reduce future risks.

4	Evaluate and identify areas of weakness related to employee skills.	Assess employee readiness, education, and training. Document and plan for updates in education or procedural changes to eliminate potential for future Incidents.
5	Report on findings and implement recommendations.	Prepare and report findings and recommendations to EHHS's Board of Trustees on any major Incidents or Breaches.

E. Each of these four elements shall be conducted as appropriate for all qualifying Incidents or Breaches. An activity log recording the timeline of Incident management shall also be completed. Reporting and documentation shall be filed and managed by EHHS's Principal or designee.

F. Audit Controls and Management
   1. On-demand documented procedures and evidence of practice should be in place for this operational policy. Appropriate audit controls and management practice examples are as follows:
      a) Archival completed Incident Reports demonstrating compliance with reporting, communication and follow-through.
      b) Executed communication plans for Incident management.
      c) Evidence of cross-departmental communication throughout the analysis, response and post-mortem processes.

G. Enforcement
   1. Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

H. Distribution
   1. This policy is to be distributed to all EHHS staff.

T-4 Acceptable Employee Use of Internet, Computers, and Network Resources

Reference(s)

- 53A-3-422 Internet and Online Access Policy Required Children's Internet Protection Act (CIPA)
- R277-515 Utah Educator Standards

I. Purpose for Policy

A. East Hollywood High School Board of Trustees permits employees to access the Internet and use EHHS computers and network resources as part of their work responsibilities.
B. The use of EHHS network resources is a privilege, not a right, and all usage must be in compliance with the accompanying administrative procedures. In general, EHHS requires responsible, decent, ethical, polite, efficient, and legal use of its network resources.
C. EHHS has also taken appropriate precautions to restrict access to inappropriate materials including filtering Internet access on all EHHS purchased devices on and off-site; however, on a global network it is impossible to guarantee that all inappropriate material will be blocked.
D. Disciplinary action may be imposed, including the revocation of network privileges, for failure to comply with this policy or its administrative procedures.
E. The purpose of this policy is to inform all employees of the guidelines that must be followed when using the EHHS's computers and network resources.

II. Authority

A. The EHHS has the right to place restrictions on the use of equipment, resources, and materials employees' access or disclose through the EHHS's Internet, computers, and network resources (collectively "electronic resources").
B. In general, all EHHS employees are responsible for the efficient, ethical, and legal utilization of the EHHS's electronic resources. Employees must therefore comply with all applicable local, state, and federal laws, board policies, and administrative procedures in their use of such resources.

III. Access to EHHS Electronic Resources

A. Employees may be given access to the EHHS's electronic resources, including an account and password. This access must not be shared, assigned, or transferred to another individual.
B. The EHHS will periodically require new registration and account information from its employees. Employees must notify the school principal of any changes in account information (address, phone, name, etc.). Once EHHS administration updates the information, the changes should start propagating to EHHS systems within 24 hours. If that does not occur, please contact the EHHS's information systems department (IT department).
C. This access has not been established as a public access service or a public forum.

IV. Privileges

A. The use of the EHHS's electronic resources is a privilege, not a right. Inappropriate use may result in disciplinary action up to and including termination, and when appropriate, a referral to legal authorities. An administrator or supervisor may limit, suspend, or revoke an employee's access to electronic resources at any time.
B. The EHHS uses monitoring systems to monitor and detect inappropriate use and may use tracking systems to track and recover lost or stolen equipment.
C. By accessing the EHHS's network resources, employees acknowledge that they have read, understand, and agree to abide by the provisions EHHS's Acceptable Use policy.

V. Acceptable Use

A. An employee's use of the EHHS's electronic resources shall be consistent with the EHHS's purpose, mission, and goals, and shall be for educational and professional purposes.
B. Incidental use of electronic resources for personal reasons is allowed provided that such use does not:
    1. Disrupt or distract from the conduct of EHHS business due to volume, timing or frequency.
    2. Interfere with the employee's duties.
    3. Violate the provisions of these administrative procedures.
    4. Involve actions which may harm or otherwise disadvantage EHHS.
    5. Any employee who "publishes" on the Internet must abide by the EHHS's approved publishing procedures.
    6. All employees are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:
        a) Be polite.
        b) Do not be abusive in your messages to others.
        c) Use appropriate language.
        d) If told by a person to stop sending messages, the sender must stop.

VI. Prohibited Uses

A. The following uses of the EHHS's electronic resources are prohibited and just cause for termination of use privileges, disciplinary action, and/or legal action.
    1. Illegal use: any use that violates, or supports the violation of, federal, state, or local laws, and/or board policy; any unauthorized use of copyrighted materials or material protected by trade secrets; any use in violation of software license agreements; any use that constitutes plagiarism.
    2. Vandalism and/or theft: any deliberate attempt to damage the hardware, software, or information residing on the EHHS's network or any other computer system attached through the Internet; violating, or attempting to violate, the integrity of private accounts, files, or programs; deliberately infecting a computer with a virus; hacking computers using any method; interfering with computer or network performance; interfering with another's ability to use equipment and systems; destroying data.

3. Commercial use: any use for commercial purposes or activities resulting in personal financial gain, including product advertisements and solicitations.

4. Offensive or harassing behavior: any use of material, whether visual or textual, that may be deemed profane, vulgar, abusive, threatening, obscene, or sexually explicit; distribution of disparaging or harassing statements including those that might incite violence or that are based on race, national origin, sex, sexual orientation, age, disability, or political or religious beliefs; posting of anonymous messages.
5. Religious or political use: any use for a religious or political purpose, including religious proselytizing and lobbying for student body elections.
6. Security violations: using an account other than your own; accessing, or attempting to access accounts, sites, servers, files, databases, or other systems for which an employee is not authorized (e.g. "hacking" or using "spyware"); spreading computer viruses; degrading or disrupting network equipment, software, or system performance; running applications or files that create a security risk; any other action that threatens the security of the EHHS's electronic resources.
7. Any employee who "publishes" on the Internet must abide by the EHHS's approved publishing procedures.
8. All employees are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:
   a) Be polite.
   b) Do not be abusive in your messages to others.
   c) Use appropriate language.
   d) If told by a person to stop sending messages, the sender must stop.
9. Unnecessary uses: downloading or streaming audio or video files, or any other files that are not directly related to ordinary course of business; forwarding or replying to chain letters, pyramid schemes, "contests" or "fast cash" schemes; and posting or sending advertisements, unauthorized solicitations, mass cross-postings, and uninvited mass mailings.
10. Tampering: any attempt to bypass state, EHHS, or school security; attempting to disable or bypass the EHHS's Internet blocking/filtering software without authorization; adding, modifying, repairing, removing, reconfiguring or tampering with any device on the EHHS's network infrastructure.

VII. Violations and Discipline

A. Authorized EHHS employees will be responsible for determining what constitutes a violation of this policy. Authorized EHHS employees have the right to intercept or read a user's email, review any material and to edit or remove any material which they believe may be unlawful, obscene, defamatory, abusive, or otherwise objectionable. If the EHHS intends to impose any discipline other than revoking privileges, the employee will be afforded appropriate due process.

B. The following processes must be followed when reporting a violation:
   1. Notify a school administrator or the EHHS's IT department.
   2. The school administrator or member of the IT department will notify the EHHS.
   3. Business Manager and the appropriate law enforcement agency if necessary.
   4. EHHS Business Manager will guide the investigation and subsequent discipline.

5. EHHS Principal and Business Manager may request assistance in the investigation from the IT department.
6. Any substantiated violation and imposed discipline will be recorded in the employee's personnel file.

C. If in the course of performing his or her job duties, a member of the IT department views an image on a computer or other electronic device that is or appears to be child pornography, state law requires the IT staff member to immediately report the finding of the image to state or local law enforcement, the Cyber Tip Line at the National Center for Missing and Exploited Children, or the Chief Information Officer.

VIII. Privacy Information

A. Nothing is private on the network. The EHHS's electronic resources are EHHS property. Employees should recognize there is no expectation of privacy as to their use of the EHHS's electronic resources. Therefore, employees shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the EHHS's electronic resources, including personal files. The EHHS reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization; and deny access to prevent unauthorized, inappropriate or illegal activity.

B. The EHHS shall cooperate fully with local, state and federal officials in any investigation concerning or related to illegal activities. In addition, under Utah's Governmental Records Access Management Act and the Federal Educational Right to Privacy Act, persons outside the EHHS may be able to request and receive information regarding an employee's communications and use of electronic resources.

IX. Ownership of Messages, Data and Documents

A. Except where required by law, all information contained in the EHHS's electronic resources are EHHS property. Therefore, all information created, sent, received, accessed or stored using these electronic resources is the property of the EHHS.

B. Upon termination of employment, EHHS is under no obligation to provide access to personal files or other information stored on the EHHS's electronic resources.

X. Security

A. Security is a high priority on computer networks because of multiple users.

B. If a security problem is identified, the user must notify the system administrator immediately. Employees must not demonstrate the problem to other users.

C. You must report any of the following to a school administrator or the IT department:
1. If you receive or obtain information to which you are not entitled.
2. If you know of any inappropriate use of the network by others.
3. If you believe the filtering software is not filtering a site or sites that should be filtered.
4. If you have information that users are using and/or accessing accounts other than their own.

XI. Filtering/Blocking Software

A. The EHHS utilizes and consistently configures filtering/blocking software to block access to sites and materials that are inappropriate, offensive, and obscene, contain pornography, or are otherwise harmful to EHHS personnel as required by federal and state law. Filtering/blocking software is continuously in effect on the EHHS's electronic resources on and off-site. The EHHS will utilize its best efforts to block access to such inappropriate sites and materials, but cannot warrant the complete effectiveness of its filtering/blocking software.

XII. Disclaimer

A. EHHS makes no warranties of any kind, whether expressed or implied, for the services it is providing. Electronic resources are provided on an "as is, as available" basis.

B. EHHS will not be responsible for any damages an employee may suffer while using its electronic resources. These damages may include but are not limited to:
   1. Loss of data resulting from delays, non-deliveries, or service interruptions caused by the system or by employee negligence, error or omission.
   2. EHHS makes no promise or warranty to maintain or update its network, or the information contained therein.
   3. EHHS may suspend or discontinue these services at any time. Use of any information obtained via the information system is at the employee's own risk.
   4. EHHS specifically denies any responsibility for the accuracy or appropriateness of information obtained through electronic resources.

T-5 Acceptable Student Use of Internet, Computers, and Network Resources

Resource(s)

- 53A-3-422 Internet and online access policy
- 53A-3-423 Process and content standards for policy
- Children's Internet Protection Act (CIPA)

I. PURPOSE

A. The purpose of this policy is to ensure all students and parents understand the rules and procedures that must be followed in order to gain access to and use EHHS's network resources. Use of EHHS's network resources is a privilege and may be revoked at any time for failure to comply with this policy or its administrative procedures.

B. EHHS's Board of Trustees and Administration permits students to have Internet access. In accordance with state and federal law. EHHS utilizes available technology protection measures to restrict students' access to Internet or online sites that contain obscene or inappropriate materials. However, on a global network it is impossible to control all materials and an industrious student may discover inappropriate information.

C. EHHS requires all students to use the school's network resources in a responsible, ethical, polite, efficient, and legal manner. To that end, teachers will instruct and supervise students on responsible use of Internet resources and proper network etiquette. A Responsible Use Contract must be signed by each student and his or her parent or guardian, annually at registration.

II. Procedures for implementation

A. EHHS has the right to, and in some instances a legal obligation to place restrictions on students' use of and access to its computer systems, computer networks, EHHS adapted tools and devices, software applications, email, and the Internet (collectively "electronic resources").

B. In general, all students are responsible for the responsible, ethical, and legal utilization of EHHS's electronic resources. When using these resources, students must comply with these administrative procedures.

III. Access to EHHS's Electronic Resources

A. Through the registration process, parents and students will attest that they have read and understand these administrative procedures and the accompanying board policy ("Responsible Use Contract").

B. Parents may terminate their student's access in accordance with Section VI.

C. At a minimum, teachers shall review these administrative procedures and other applicable rules and regulations with students on an annual basis, but teachers are encouraged to discuss appropriate use guidelines with students on a regular basis when they are using the school's electronic resources.

D. After enrolling, all students will be provided a password in order to access the school's electronic resources.

IV. Privileges

A. The use of EHHS's electronic resources is a privilege, not a right. Inappropriate use may result in a loss of network privileges, disciplinary action, and/or referral to legal authorities. The system administrators have the authority to close an account at any time. An administrator or faculty member may request the system administrator deny, revoke, or suspend a specific user's access and/or his or her user accounts.
B. By accessing the school's network resources, students acknowledge that they have read, understand, and agree to comply EHHS's Acceptable Student Use of Internet, Computer, and Network Resources Policy.

V. Acceptable Use

A. Student's use of EHHS's electronic resources shall be for educational purposes only, which includes accessing and sharing information with teachers and other students, storing files, conducting research, and collaborating on projects with others.
    1. In some instances, students may be directed by their teachers to use EHHS's electronic resources in conjunction with their curriculum, an assessment, or a behavior support program.
B. Students are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:
    1. Be polite.
    2. Do not be abusive in your messages to others.
    3. Use appropriate language.
    4. If told by a person to stop sending messages, the sender must stop.

VI. Prohibited Uses

A. Illegal use: any use that violates, or supports the violation of, federal, state, or local laws, board policy, school rules, and/or the student code of conduct (including any form of cyber-bullying); use of copyrighted materials or material protected by trade secrets without appropriate authorization; any use in violation of software license agreements; and any use that constitutes plagiarism.
B. Vandalism and/or theft: any deliberate attempt to damage the hardware, software, or information resident on EHHS's network or any other computer system attached through the Internet; violating, or attempting to violate, the integrity of private accounts, files, or programs; deliberately infecting a computer with a virus; hacking computers using any method; interfering with computer or network performance; interfering with another's ability to use equipment and systems; destroying data.
C. Commercial use: any use for commercial purposes or activities resulting in personal financial gain, including product advertisements and solicitations.
D. Commercial use: any use for commercial purposes or activities resulting in personal financial gain, including product advertisements and solicitations.
E. Offensive or harassing behavior: any use of material, whether visual or textual, that may be deemed profane, vulgar, abusive, threatening, obscene, or sexually explicit; distribution of disparaging or harassing statements including those that might incite violence or that are based on race, color, pregnancy, gender identity, genetic information, national origin, sex, sexual orientation, age, disability, or political or religious beliefs; posting of anonymous messages.
F. Religious or political use: any use for a religious or political purpose, including religious proselytizing and lobbying for student body elections.
G. Security violations: using an account other than your own; accessing, or attempting to access accounts, sites, servers, files, databases, or other systems for which a student

is not authorized (e.g. “hacking” or using “spyware”); spreading computer viruses; degrading or disrupting network equipment, software, or system performance; running applications or files that create a security risk; any other action that threatens the security of EHHS’s electronic resources.

H. Disseminating or accessing confidential information: transmitting confidential information about other individuals; violating the privacy of others by reading or posting e-mail or other private communications without obtaining the appropriate consent; providing personal addresses, phone numbers, or financial information in any network communication whether that information belongs to the student user or any other individual unless it is related to an appropriate education objective in the curriculum.

I. Unnecessary uses: downloading or streaming audio or video files, or any other files that are not directly related to course curriculum; playing non-educational Internet games; accessing or using services on the Internet that impose a fee on the student.

J. Tampering: any attempt to bypass state, EHHS, or school security; attempting to disable or bypass EHHS’s Internet blocking/filtering software without authorization; adding, modifying, repairing, removing, reconfiguring, or tampering with any device on EHHS’s network infrastructure.

VII. Discipline and Termination of Accounts

A. EHHS’s principal will be responsible to determine what constitutes a violation of these procedures. Authorized school employees have the right to intercept or read a student’s email, review any material, edit or remove any material which they believe may be unlawful, obscene, defamatory, abusive, or otherwise objectionable.

B. If EHHS’s administration intends to impose any discipline, other than revoking privileges for the remainder of the school year, the user will be afforded appropriate due process.

C. An account will be terminated when:
   1. The student’s parent and/or guardian makes a request in writing to the principal that the account be terminated.
   2. Any authorized EHHS employee believes the account should be terminated.
   3. A student leaves EHHS.

VIII. Privacy Information

A. Nothing is private on the network. A student has no expectation of privacy as to his or her communications on or uses of the Internet. Frequently internet sites maintain records that can be subpoenaed to identify what the user has been viewing and downloading on the Internet.

B. EHHS reserves the right to monitor whatever a user does on the network.

IX. Security

A. Security is a high priority on EHHS’s computer networks.

B. If a security problem is identified, the user must notify the system administrator immediately. Students should not demonstrate the problem to other users.
   1. Users may not use the Internet to discuss or disseminate information regarding security problems or how to gain unauthorized access to sites, servers, files, etc.
   2. Do not share passwords with other users, and change passwords frequently.
   3. Do not leave an electronic workstation without logging out of the network.

C. You must report any of the following to a teacher or administrator:
   1. If you receive or obtain information to which you are not entitled.

2. If you know of any inappropriate use of the network by others.
3. If you believe the filtering software is not filtering a site or sites that should be filtered under this agreement.

X. Disclaimer

A. EHHS makes no warranties of any kind, whether expressed or implied, for the services it is providing. Electronic resources are provided on an "as is, as available" basis.
B. EHHS will not be responsible for any damages a student may suffer while using its electronic resources. These damages may include but are not limited to: loss of data resulting from delays, non-deliveries, or service interruptions caused by the system or by an individual's negligence, error or omission.
C. EHHS makes no promise or warranty to maintain or update its network, or the information contained therein.
D. EHHS may suspend or discontinue these services at any time. Use of any information obtained via the information system is at the student's own risk.
E. EHHS specifically denies any responsibility for the accuracy or appropriateness of information obtained through electronic resources.

XI. Filtering/Blocking Software

A. In accordance with state law and the Children's Internet Protection Act, EHHS utilizes and consistently configures filtering/blocking software to block access to sites and materials that are inappropriate, offensive, obscene, contain pornography, or are otherwise harmful to students.
B. EHHS will utilize its best efforts to block access to such sites and materials, but cannot guarantee the complete effectiveness of its filtering/blocking software.

East Hollywood High School
Data Governance Plan

1 PURPOSE

Data governance is an organizational approach to data and information management that is formalized as a set of policies and procedures that encompass the full life cycle of data; from acquisition, to use, to disposal. East Hollywood High School Board of Trustees takes seriously its moral and legal responsibility to protect student privacy and ensure data security.

2 SCOPE AND APPLICABILITY

This policy is applicable to all employees, temporary employees, and contractors of the Agency. The policy must be used to assess agreements made to disclose data to third-parties. This policy is also used to assess the risk of conducting business. In accordance with Agency policy and procedures, this policy will be reviewed and adjusted on an annual basis or more frequently, as needed. This policy is designed to ensure only authorized disclosure of confidential information. The following 8 subsections provide data governance policies and processes for *East Hollywood High School.*

1. Data Advisory Groups
2. Non-Disclosure Assurances for Employees
3. Data Security and Privacy Training for Employees
4. Data Disclosure
5. Data Breach
6. Record Retention and Expungement
7. Data Quality
8. Transparency

Furthermore, *EHHS* Data Governance Plan works in conjunction with the Agency Information Security Policy, which:

1. Designates *EHHS* as the steward for all confidential information maintained within the school.
2. Designates Data Stewards access for all confidential information.
3. Requires Data Stewards to maintain a record of all confidential information that they are responsible for.
4. Requires Data Stewards to manage confidential information according to this policy and all other applicable policies, standards and plans.
5. Complies with all legal, regulatory, and contractual obligations regarding privacy of Agency data. Where such requirements exceed the specific stipulation of this policy, the legal, regulatory, or contractual obligation shall take precedence.
6. Provides the authority to design, implement, and maintain privacy procedures meeting *EHHS* standards concerning the privacy of data in motion, at rest and processed by related information systems.
7. Ensures that all *EHHS* board members, employees, contractors, and volunteers comply with the policy and undergo annual privacy training.
8. Provides policies and process for

- Systems administration,
- Network security,
- Application security,
- Endpoint, server, and device Security
- Identity, authentication, and access management,
- Data protection and cryptography
- Monitoring, vulnerability, and patch management
- High availability, disaster recovery, and physical protection
- Incident Responses
- Acquisition and asset management, and
- Policy, audit, e-discovery, and training.

3 DATA ADVISORY GROUPS

3.1 STRUCTURE

EHHS has a three-tiered data governance structure to ensure that data is protected at all levels of Utah's educational system.

3.2 GROUP MEMBERSHIP

Membership in the groups require board approval. Group membership is for two years. If individual members exit the group prior to fulfilling their two-year appointment, the board may authorize EHHS's Principal/Director to appoint a replacement member.

3.3 INDIVIDUAL AND GROUP RESPONSIBILITIES

The tables listed on the following page outlines *EHHS* individual staff and advisory group responsibilities.

3.3.1 Table 1. Individual *EHHS* Staff Responsibilities

Role	Responsibilities
LEA Student Data Manager (Principal/Director)	1. authorize and manage the sharing, outside of the education entity, of personally identifiable student data from a cumulative record for the education entity 2. act as the primary local point of contact for the state student data officer. 3. A student data manager may share personally identifiable student data that are: a. of a student with the student and the student's parent b. required by state or federal law c. in an aggregate form with appropriate data redaction techniques applied d. for a school official e. for an authorized caseworker or other representative of the Department of Human Services or the Juvenile Court f. in response to a subpoena issued by a court. g. directory information h. submitted data requests from external researchers or evaluators, 4. A student data manager may not share personally identifiable student data for the purpose of external research or evaluation. 5. Create and maintain a list of all LEA staff that have access to personally identifiable student data. 6. Ensure annual LEA level training on data privacy to all staff members, including volunteers. Document all staff names, roles, and training dates, times, locations, and agendas.
IT Systems Security Manager (Bobby James)	1. Acts as the primary point of contact for state student data security administration in assisting the board to administer this part; 2. ensures compliance with security systems laws throughout the public education system, including: a. providing training and support to applicable *EHHS* employees; and b. producing resource materials, model plans, and model forms for LEA systems security; 3. investigates complaints of alleged violations of systems breaches; 4. provides an annual report to the board on *EHHS's* systems security needs
Educators	EHHS's Director of Special Education, School Counselor, Registrar, and Vice Principal shall serve as a group member on the school's Data Advisory Board.
Other	Other members on the Data Advisory Board may include and are not limited to the following: • Board of Trustee Members • Director of Finance • Outside educational agency that EHHS's Board of Trustees and school administration deemed as a valued member to the Data Advisory Board. Additional members may include, but are not limited to the following: Data Specialist contractor's and volunteers

4 EMPLOYEE NON-DISCLOSURE ASSURANCES

Employee non-disclosure assurances are intended to minimize the risk of human error and misuse of information.

4.1 SCOPE

All *EHHS* board members, employees, contractors and volunteers must sign and obey the EHHS Employee Non-Disclosure Agreement (See Appendix A), which describes the permissible uses of state technology and information.

4.2 NON-COMPLIANCE

Non-compliance with the agreements shall result in consequences up to and including removal of access to *EHHS* network; if this access is required for employment, employees and contractors may be subject to dismissal.

4.3 NON-DISCLOSURE ASSURANCES

All student data utilized by *EHHS* is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and Utah statute. This policy outlines the way *EHHS* staff is to utilize data and protect personally identifiable and confidential information. A signed agreement form is required from all *EHHS* staff to verify agreement to adhere to/abide by these practices and will be maintained in *EHHS* Principal/Director. All *EHHS* employees (including contract or temporary) will:

1. Complete a Security and Privacy Fundamentals Training.
2. Complete a Security and Privacy Training for Researchers and Evaluators, if your position is a research analyst or if requested by EHHS's Principal/Director.
3. Consult with *EHHS* internal data owners when creating or disseminating reports containing data.
4. Use password-protected state-authorized computers when accessing any student-level or staff-level records.
5. NOT share individual passwords for personal computers or data systems with anyone.
6. Log out of any data system/portal and close the browser after each use.
7. Store sensitive data on appropriate-secured location. Unsecured access and flash drives, DVD, CD-ROM or other removable media, or personally owned computers or devices are not deemed appropriate for storage of sensitive, confidential or student data.
8. Keep printed reports with personally identifiable information in a locked location while unattended, and use the secure document destruction service provided at *EHHS* when disposing of such records.
9. NOT share personally identifying data during public presentations, webinars, etc. If users need to demonstrate child/staff level data, demo records should be used for such presentations.
10. Redact any personally identifiable information when sharing sample reports with general audiences, in accordance with guidance provided by the student data manager, found in Appendix B (Protecting PII in Public Reporting).
11. Take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.

12. Delete files containing sensitive data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties.
13. NOT use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If users receive an email containing such information, they will delete the screenshots/text when forwarding or replying to these messages. If there is any doubt about the sensitivity of the data the Student Data Privacy Manager should be consulted..
14. Use secure methods when sharing or transmitting sensitive data. The approved method is *EHHS's* Secure File Transfer Protocol (SFTP) website. Also, sharing within secured server folders is appropriate for *EHHS* internal file transfer.
15. NOT transmit child/staff-level data externally unless expressly authorized in writing by the data owner and then only transmit data via approved methods such as described in item ten.
16. Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.

4.4 DATA SECURITY AND PRIVACY TRAINING

4.4.1 Purpose

EHHS will provide a range of training opportunities for all *EHHS* staff, including volunteers, contractors and temporary employees with access to student educational data or confidential educator records in order to minimize the risk of human error and misuse of information.

4.4.2 Scope

All *EHHS* board members, employees, and contracted partners.

4.4.3 Compliance

New employees that do not comply may not be able to use *EHHS* networks or technology.

4.4.4 Policy

1. Within the first week of employment, all *EHHS* board members, employees, and contracted partners must sign and follow EHHS Employee Acceptable Use Policy, which describes the permissible uses of state technology and information.
2. New employees that do not comply may not be able to use *EHHS* networks or technology. Within the first week of employment, all *EHHS* board members, employees, and contracted partners also must sign and obey EHHS Employee Non-Disclosure Agreement, which describes appropriate uses and the safeguarding of student and educator data.
3. All current *EHHS* board members, employees, and contracted partners are required to participate in an annual Security and Privacy Fundamentals Training Curriculum within 60 days of the adoption of this rule.
4. *EHHS* requires a targeted Security and Privacy Training for Data Stewards and IT staff for other specific groups within the agency that collect, store, or disclose data. The Chief Privacy Officer will identify these groups. Data and Statistics Coordinator will determine the annual training topics for these targeted groups based on *EHHS* training needs.
5. Participation in the training as well as a signed copy of the Employee Non-Disclosure Agreement will be annually monitored by supervisors. Supervisors and the board secretary will annually report all *EHHS* board members, employees, and contracted partners who do not have these requirements completed to the IT Security Manager.

5 DATA DISCLOSURE

5.1 PURPOSE

Providing data to persons and entities outside of EHHS increases transparency, promotes education in Utah, and increases knowledge about Utah public education. This policy establishes the protocols and procedures for sharing data maintained by *{INSERT LEA NAME HERE}*. It is intended to be consistent with the disclosure provisions of the federal Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, 34 CFR Part 99 and Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401.

5.2 POLICY FOR DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

5.2.1 Student or Student's Parent/Guardian Access

Parents are advised that the records maintained by *EHHS* are provided to *EHHS* by the school district in which their student is/was enrolled, and access to their student's record can be obtained from the student's school district. In accordance with FERPA regulations 20 U.S.C. § 1232g (a)(1) (A) (B) (C) and (D), LEAs will provide parents with access to their child's education records, or an eligible student access to his or her own education records (excluding information on other students, the financial records of parents, and confidential letters of recommendation if the student has waived the right to access), within 45 days of receiving an official request. LEAs and *EHHS* is not required to provide data that it does not maintain, nor is *EHHS* required to create education records in response to an eligible student's request.

5.2.2 Third Party Vendor

Third party vendors may have access to students' personally identifiable information if the vendor is designated as a "school official" as defined in FERPA, 34 CFR §§ 99.31(a)(1) and 99.7(a)(3)(iii). A school official may include parties such as: professors, instructors, administrators, health staff, counselors, attorneys, clerical staff, trustees, members of committees and disciplinary boards, and a contractor, consultant, volunteer or other party to whom the school has outsourced institutional services or functions.

All third-party vendors contracting with *EHHS* must be compliant with Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401. Vendors determined not to be compliant may not be allowed to enter into future contracts with *EHHS* without third-party verification that they are compliant with federal and state law, and board rule.

5.2.3 Internal Partner Requests

Internal partners to *EHHS* include LEA and school officials that are determined to have a legitimate educational interest in the information. All requests shall be documented in *EHHS's* data request ticketing system.

5.2.4 Governmental Agency Requests

EHHS may not disclose personally identifiable information of students to external persons or organizations to conduct research or evaluation that is not directly related to a state or federal program reporting requirement, audit, or evaluation. The requesting governmental agency must provide evidence the federal or state requirements to share data in order to satisfy FERPA disclosure exceptions to data without consent in the case of a federal or state

a) reporting requirement
b) audit
c) evaluation

The Coordinator of Data and Statistics will ensure the proper data disclosure avoidance are included if necessary. An Interagency Agreement must be reviewed by legal staff and must include "FERPA-Student Level Data Protection Standard Terms and Conditions or Required Attachment Language."

5.3 Policy for External disclosure of Non-Personally Identifiable Information (PII)

5.3.1 Scope

External data requests from individuals or organizations that are not intending on conducting external research or are not fulfilling a state or federal reporting requirement, audit, or evaluation.

5.3.2 Student Data Disclosure Risk Levels

EHHS has determined four levels of data requests with corresponding policies and procedures for appropriately protecting data based on risk: Low, Medium, and High. The Coordinator of Data and Statistics will make final determinations on classification of student data requests risk level.

5.3.2.1 Low-Risk Data Request Process

Definition: High-level aggregate data
Examples:

- Graduation rate by year for the state
- Percent of third-graders scoring proficient on the SAGE ELA assessment

Process: Requester creates a ticket, Data Request forwarded to appropriate Data Steward. Data Steward fulfills request and saves the dataset in a secure folder managed by the Coordinator of Data and Statistics. The Data Steward closes the ticket.

5.3.2.2 Medium-Risk Data Request Process

Definition: Aggregate data, but because of potentially low n-sizes, the data must have disclosure avoidance methods applied.

Examples:

- Graduation rate by year and LEA
- Percent of third-graders scoring proficient on the SAGE ELA assessment by school
- Child Nutrition Program Free or Reduced Lunch percentages by school

Process: Requester creates a ticket, Data Request forwarded to appropriate Data Steward, Data Steward fulfills request, applies appropriate disclosure avoidance techniques, and sends to another Data Steward for Quality Assurance (ensuring student data protection). If it passes QA, data are sent to requester and saves the dataset in a secure folder managed by the Coordinator of Data and Statistics. Data Steward closes the ticket. If it does not pass QA, the data are sent back to the Data Steward for modification.

5.3.2.3 High-Risk Data Request Process

Definition: Student-level data that are de-identified.

Examples:

- De-identified student-level graduation data

- De-identified student-level SAGE ELA assessment scores for grades 3-6.

Process: Requester creates a ticket, Data Request forwarded to Data and Statistic Coordinator for review. If the request is approved, an MOA is drafted and sent to legal, placed on the board consent calendar, reviewed by the Superintendent, sent to the Purchasing/Contract Manager, sent to Coordinator or Data and Statistics, appropriate Data Steward fulfills request, de-identifies data as appropriate, and sends to another Data Steward for Quality Assurance (ensuring student data protection). If it passes QA, data are sent to requester and saves the dataset in a secure folder managed by the Coordinator of Data and Statistics. The Data Steward closes the ticket. If it does not pass QA, the data are sent back to the Data Steward for modification.

5.4 Data Disclosure to a Requesting External Researcher or Evaluator

Responsibility: The Coordinator of Data and Statistics will ensure the proper data are shared with external researcher or evaluator to comply with federal, state, and board rules. *EHHS* may not disclose personally identifiable information of students to external persons or organizations to conduct research or evaluation that is not directly related to a state or federal program audit or evaluation. Data that do not disclose PII may be shared with external researcher or evaluators for projects unrelated to federal or state requirements if:

1. *EHHS* Principle/Director and or Business Manager/Director, or board member sponsors an external researcher or evaluator request.
2. Student data are not PII and are de-identified through disclosure avoidance techniques and other pertinent techniques as determined by the Coordinator of Data and Statistics.
3. Researchers and evaluators shall supply *EHHS* a copy of any publication or presentation that uses *EHHS* data 10 business days prior to any publication or presentation.

6 Data Breach

6.1 Purpose

Establishing a plan for responding to a data breach, complete with clearly defined roles and responsibilities, will promote better response coordination and help educational organizations shorten their incident response time. Prompt response is essential for minimizing the risk of any further data loss and, therefore, plays an important role in mitigating any negative consequences of the breach, including potential harm to affected individuals.

6.2 Policy

EHHS shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, *EHHS* staff shall follow industry best practices outlined in the Agency IT Security Policy for responding to the breach. Further, *EHHS* shall follow best practices for notifying affected parties, including students, in the case of an adult student, or parents or legal guardians, if the student is not an adult student.

Concerns about security breaches must be reported immediately to the IT security manager who will collaborate with appropriate members of EHHS executive team to determine whether a security breach has occurred. If EHHS data breach response team determines that one or more employees or contracted partners have substantially failed to comply with *EHHS*'s Agency IT Security Policy and relevant privacy policies, they will identify appropriate consequences, which may include termination of employment or a contract and further legal action. Concerns about security breaches that involve the IT Security Manager must be reported immediately to EHHS's Principal/Director.

EHHS will provide and periodically update, in keeping with industry best practices, resources for Utah LEAs in preparing for and responding to a security breach. EHHS will make these resources available on its website.

7 RECORD RETENTION AND EXPUNGEMENT

7.1 PURPOSE

Records retention and expungement policies promote efficient management of records, preservation of records of enduring value, quality access to public information, and data privacy.

7.2 SCOPE

EHHS board members and staff.

7.3 POLICY

EHHS staff, Utah LEAs and schools shall retain and dispose of student records in accordance with Section 63G-2-604, 53A-1-1407, and shall comply with active retention schedules for student records per Utah Division of Archive and Record Services.

In accordance with 53A-1-1407, EHHS shall expunge student data that is stored upon request of the student if the student is at least 23 years old. *EHHS* may expunge medical records and behavioral test assessments. *EHHS* will not expunge student records of grades, transcripts, a record of the student's enrollment or assessment information. *EHHS* staff will collaborate with Utah State Achieves and Records Services in updating data retention schedules.

EHHS's maintained student-level discipline data will be expunged after three years.

8 QUALITY ASSURANCES AND TRANSPARENCY REQUIREMENTS

8.1 PURPOSE

Data quality is achieved when information is valid for the use to which it is applied, is consistent with other reported data and users of the data have confidence in and rely upon it. Good data quality does

not solely exist with the data itself, but is also a function of appropriate data interpretation and use and the perceived quality of the data. Thus, true data quality involves not just those auditing, cleaning and reporting the data, but also data consumers. Data quality at is addressed in five areas:

8.1.1 Data Governance Structure

EHHS data governance policy is structured to encourage the effective and appropriate use of educational data. EHHS data governance structure centers on the idea that data is the responsibility of all *EHHS* sections and that data driven decision making is the goal of all data collection, storage, reporting and analysis. Data driven decision making guides what data is collected, reported and analyzed.

8.1.2 Data Requirements and Definitions

Clear and consistent data requirements and definitions are necessary for good data quality. On the data collection side, *EHHS* communicates data requirements and definitions to LEAs through the Data Clearinghouse Update Transactions documentation (see http://www.schools.utah.gov/computerservices/Data-Clearinghouse.aspx). *EHHS* also communicates with IT staff regularly, at monthly Data Warehouse Group meetings and at biannual Data Conferences. Where possible, *EHHS* program specialists are invited to these meetings and the same guidance is given to the appropriate LEA program directors.

On the data reporting side, the production and presentation layers provide standard data definitions and business rules. Data Stewards coordinate data releases through the Data Stewards Group meetings. All data released includes relevant data definitions, business rules, and are date stamped. Further, Data and Statistics produces documentation, trainings and FAQs on key statistics and reports, such as AYP, graduation rate and class size.

8.1.3 Data Collection

Data elements should be collected only once—no duplicate data collections are permitted. Where possible, data is collected at the lowest level available (i.e. at the student/teacher level). Thus, there are no aggregate data collections if the aggregate data can be derived or calculated from the detailed data. For all new data collections, *EHHS will* provide clear guidelines for data collection and the purpose of the data request.

8.1.4 Data Auditing

Data and Statistics Data Analysts perform regular and ad hoc data auditing. They analyze data in the warehouse for anomalies, investigate the source of the anomalies, and work with IT and/or LEAs in explaining and/or correcting the anomalies. Data Analysts also work with School Finance to address findings from the Auditors.

8.1.5 Quality Control Checklist

Checklists have been proven to increase quality (See Appendix C). Therefore, before releasing high-risk data, Data Stewards and Data Analysts must successfully complete the data release checklist in three areas: reliability, validity and presentation.

9 DATA TRANSPARENCY

Annually, *EHHS* will publically post:

- *EHHS* data collections

- Metadata Dictionary as described in Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401

10 APPENDIX

Appendix A.

EHHS Employee Non-Disclosure Agreement

As an employee of East Hollywood High School, I hereby affirm that: (Initial)

_____ I have read the Employee Non-Disclosure Assurances attached to this agreement form and read and reviewed Data Governance Plan *EHHS* policies. These assurances address general procedures, data use/sharing, and data security.

_____ I will abide by the terms of EHHS's policies and its subordinate process and procedures;

_____ I grant permission for the manual and electronic collection and retention of security related information, including but not limited to photographic or videotape images, of your attempts to access the facility and/or workstations.

Trainings

_____ I have completed Data Security and Privacy Fundamentals Training.

_____ I will complete *EHHS's* Data Security and Privacy Fundamentals Training within 30 days.

Using *EHHS* Data and Reporting Systems

_____ I will use a password-protected computer when accessing data and reporting systems, viewing child/staff records, and downloading reports.

_____ I will not share or exchange individual passwords, for either personal computer(s) or *EHHS* system user accounts, with *EHHS* staff or participating program staff.

_____I will log out of and close the browser after each use of *EHHS* data and reporting systems.

_____I will only access data in which I have received explicit written permissions from the data owner.

_____I will not attempt to identify individuals, except as is required to fulfill job or volunteer duties, or to publicly release confidential data;

Handling Sensitive Data

_____ I will keep sensitive data on password-protected state-authorized computers.

_____ I will keep any printed files containing personally identifiable information in a locked location while unattended.

_____ I will not share child/staff-identifying data during public presentations, webinars, etc. I understand that dummy records should be used for such presentations.

_____ I will delete files containing sensitive data after working with them from my desktop, or move them to a secured *EHHS* server.

Reporting & Data Sharing

_____ I will not redisclose or share any confidential data analysis except to other authorized personnel without EHHS's expressed written consent.

_____ I will not publically publish any data without the approval of the Superintendent.

_____ I will take steps to avoid disclosure of personally identifiable information in state-level reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.

_____ I will <u>not</u> use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If I receive an email containing such information, I will delete the screenshots/text when forwarding or replying to these messages.

_____I will not transmit child/staff-level data externally unless explicitly authorized in writing.

_____ I understand that when sharing child/staff-identifying data with authorized individuals, the only approved methods are phone calls or *EHHS's* Secure File Transfer Protocol (SFTP). Also, sharing within secured server folders is appropriate for *EHHS* internal file transfer.

_____ I will immediately report any data breaches, suspected data breaches, or any other suspicious activity related to data access to my supervisor and EHHS Information Security Officer. Moreover, I acknowledge my role as a public servant and steward of child/staff information, and affirm that I will handle personal information with care to prevent disclosure.

Consequences for Non-Compliance

_____ I understand that access to EHHS network and systems can be suspended based on any violation of this contract or risk of unauthorized disclosure of confidential information;

_____I understand that failure to report violation of confidentiality by others is just as serious as my own violation and may subject me to personnel action, including termination.

Termination of Employment

_____I agree that upon the cessation of my employment from *{INSERT LEA NAME HERE}*, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of *EHHS* without the prior written permission of EHHS's Principal/Director.

Print Name: _____
Signed: _____
Date: _____

Appendix B.

Protecting PII in Public Reporting

Data Gateway Statistical Reporting Method for Protecting PII

Public education reports offer the challenge of meeting transparency requirements while also meeting legal requirements to protect each student's personally identifiable information (PII). Recognizing this, the reporting requirements state that subgroup disaggregation of the data may not be published if the results would yield personally identifiable information about an individual student. While the data used by EHHS, the data made available to the public is masked to avoid unintended disclosure of personally identifiable information at summary school, LEA, or state-level reports.

This is done by applying the following statistical method for protecting PII.

1. Underlying counts for groups or subgroups totals are not reported.
2. If a reporting group has 1 or more subgroup(s) with 10 or fewer students.
    - The results of the subgroup(s) with 10 or fewer students are recoded as "N<10"
    - For remaining subgroups within the reporting group
        1. For subgroups with 300 or more students, apply the following suppression rules.
            1. Values of 99% to 100% are recoded to ≥99%
            2. Values of 0% to 1% are recoded to ≤1%
        2. For subgroups with 100 or more than but less than 300 students, apply the following suppression rules.
            1. Values of 98% to 100% are recoded to ≥98%
            2. Values of 0% to 2% are recoded to ≤2%
        3. For subgroups with 40 or more but less than 100 students, apply the following suppression rules.
            1. Values of 95% to 100% are recoded to ≥95%
            2. Values of 0% to 5% are recoded to ≤5%
        4. For subgroups with 20 or more but less than 40 students, apply the following suppression rules.
            1. Values of 90% to 100% are recoded to ≥90%
            2. Values of 0% to 10% are recoded to ≤10%
            3. Recode the percentage in all remaining categories in all groups into intervals as follows (11-19,20-29,…,80-89)
        5. For subgroups with 10 or more but less than 20 students, apply the following suppression rules.
            1. Values of 80% to 100% are recoded to ≥80%
            2. Values of 0% to 20% are recoded to ≤20%
            3. Recode the percentage in all remaining categories in all groups into intervals as follows (20-29,30-39,…,70-79)

Appendix C.

Quality Control Checklist

Reliability (results are consistent)

1. Same definitions were used for same or similar data previously reported **or** it is made very clear in answering the request how and why different definitions were used
2. Results are consistent with other reported results **or** conflicting results are identified and an explanation provided in request as to why is different
3. All data used to answer this particular request was consistently defined (i.e. if teacher data and student data are reported together, are from the same year/time period)
4. Another *EHHS* data steward could reproduce the results using the information provided in the metadata

Validity (results measure what are supposed to measure, data addresses the request)

5. Request was clarified
6. Identified and included all data owners that would have a stake in the data used
7. Data owners approve of data definitions and business rules used in the request
8. All pertinent business rules were applied
9. Data answers the intent of the request (intent ascertained from clarifying request)
10. Data answers the purpose of the request (audience, use, etc.)
11. Limits of the data are clearly stated
12. Definitions of terms and business rules are outlined so that a typical person can understand what the data represents

Presentation

13. Is date-stamped
14. Small n-sizes and other privacy issues are appropriately handled
15. Wording, spelling and grammar are correct
16. Data presentation is well organized and meets the needs of the requester
17. Data is provided in a format appropriate to the request
18. A typical person could not easily misinterpret the presentation of the data

EAST HOLLYWOOD HIGH SCHOOL

Data Ownership and Access Policy

A. East Hollywood High School will require a signed and dated written request, which must include the person's name, address, phone number, student's name, student identification number (SID), relationship to the student, items requested for review, and reason for making the request.

B. EHHS will require proof of identity and relationship to the student before access to records is granted.

C. Requests for access to any EHHS secure materials will require a signed security/confidentiality agreement prior to inspection.

D. Any proper request for access to inspect and review any personally identifiable data by the eligible student or the student's parents will be granted without unnecessary delay and no more than 45 days after the request is made and the right to access is established by proof of identity and a signed security/confidentiality agreement, if requesting secure materials.

E. If any record includes data on more than one child, the parents shall be allowed to inspect and review only those records relevant to their child.

F. Parents shall be provided a response to reasonable requests for explanation or interpretation of the data.

G. Parents and students, when applicable, have the right to a due process hearing to challenge the content of their child's record or to ensure that the records are accurate and in no way violate the student's right to privacy.

EAST HOLLYWOOD HIGH SCHOOL

Family Educational Rights and Privacy Act (FERPA)
Notice for Directory Information

The *Family Educational Rights and Privacy Act* (FERPA), a Federal law, requires that East Hollywood High School, with certain exceptions, obtain your written consent prior to the disclosure of personally identifiable information from your child's education records. However, EHHS may disclose appropriately designated "directory information" without written consent, unless you have advised the EHHS to the contrary in accordance with procedures. The primary purpose of directory information is to allow the EHHS to include this type of information from your child's education records in certain school publications. Examples include:

- A playbill, showing your student's role in a drama production;
- The annual yearbook;
- Honor roll or other recognition lists;
- Graduation programs; and
- Sports activity sheets, such as for wrestling, showing weight and height of team members.

Directory information, which is information that is generally not considered harmful or an invasion of privacy if released, can also be disclosed to outside organizations without a parent's prior written consent. Outside organizations include, but are not limited to, companies that manufacture class rings or publish yearbooks. In addition, two federal laws require local educational agencies (LEAs) receiving assistance under the *Elementary and Secondary Education Act of 1965* (ESEA) to provide military recruiters, upon request, with the following information – names, addresses and telephone listings – unless parents have advised the EHHS that they do not want their student's information disclosed without their prior written consent. [1]

If you do not want EHHS to disclose directory information from your child's education records without your prior written consent, you must notify the school in writing by [**insert date**]. EHHS has designated the following information as directory information:

-Student's name
-Address
-Telephone listing
-Electronic mail address
-Photograph
-Date and place of birth
-Major field of study
-Dates of attendance
-Grade level
-Participation in officially recognized activities and sports
-Weight and height of members of athletic teams
-Degrees, honors, and awards received
-The most recent educational agency or institution attended
-Student ID number, user ID, or other unique personal identifier used to communicate in electronic systems that cannot be used to access education records without a PIN, password, etc. (A student's SSN, in whole or in part, cannot be used for this purpose.)

[1] These laws are: Section 9528 of the Elementary and Secondary Education Act (20 U.S.C. § 7908) and 10 U.S.C. § 503(c).

East Hollywood High School

CONTRACTORS STANDARD TERMS AND CONDITIONS
FERPA – STUDENT LEVEL DATA PROTECTION

The services or functions included in the State of Utah Contract involve the CONTRACTOR obtaining or using education records or personally identifiable information. Utah State Board of Education ("USBE") is subject to Federal Education Records Privacy Act ("FERPA") 20 U.S.C. § 1232g, and its implementing regulations, 34 C.F.R. Part 99, which generally requires written consent for disclosure of educational record or personally identifiable information to third parties.

Written consent is not required for school officials. FERPA provides a contractor, consultant, volunteer, or other outside party may be treated as a school official if the contracting party is: (a) providing services or functions that the USBE would otherwise use employees, (b) under the direct control of USBE with respect to the use and maintenance of education records and personally identifiable information, (c) subject to the requirements of 34 C.F.R. 99.33(a), and (d) limiting access within the Vendor's organization to those who have a legitimate educational interest. 34 C.F.R 99.31(a)(1)(i)(B).

USBE and CONTRACTOR desire to have CONTRACTOR treated as a school official within the FERPA exception in 34 C.F.R. 99.31(a)(1)(i)(B) and to comply with state and federal student and family privacy laws. To protect the privacy of students and parent data, USBE and CONTRACTOR ("Parties") include this Attachment to the Contract.

The Parties agree as follows:

1. The term of this Attachment shall remain in effect through the duration of the Contract.
2. The following definitions apply to the Attachment:
    a. "Education records" includes all information accessed, collected, stored, processed, disclosed, de-identified, created, or used by Vendor, including metadata and personally identifiable information, in relation to the Agreement.
    b. "Metadata" includes all information created manually or automatically to provide meaning or context to other data.
    c. "Personally Identifiable Information" or "PII" includes both direct identifiers (such as a student's or other family member's name, address, student number, or biometric number) and indirect identifiers (such as a student's date of birth, place of birth, or mother's maiden name). Indirect identifiers that constitute PII also include metadata about student interaction with an app or service, or other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

3. CONTRACTOR agrees that all data files, including derivative files, and all data files resulting from merges, matches, or other uses of education records provided or obtained pursuant to the Contract are subject to this agreement.
4. CONTRACTOR's services provided to USBE are services for which USBE would otherwise use employees.
5. CONTRACTOR is a party acting for USBE, who has direct control of the use and maintenance of education records. All education records are in the legal and rightful custody and control of USBE. CONTRACTOR acquires no rights or licenses to use the education records for any other purpose than for performing the services set forth in the Interagency Agreement.
6. CONTRACTOR has a legitimate educational interest in the education records based upon the Contract.
7. CONTRACTOR shall limit access within its organization to individuals whom CONTRACTOR has determined to have legitimate educational interests in the education records.
    a. CONTRACTOR shall require a non-disclosure agreement be signed by those individuals within its organization that CONTRACTOR determines will have access to the education records because the individuals have a legitimate educational interest in the education records.
    b. CONTRACTOR shall maintain past and current lists of all individuals to whom it has determined to allow access to education records because the individuals have legitimate educational interest in the education records.
    c. CONTRACTOR shall maintain each non-disclosure agreement signed by its employees at its facility and shall permit inspection of the same by the Board, upon request.
    d. CONTRACTOR shall maintain an audit trail for the duration of this contract, which reflects the granting and revoking of access privileges. A copy of this audit trail may be requested by USBE from Contractor at any time and shall be provided within 10 days of the USBE request.
    e. CONTRACTOR shall further notify the Board in writing within 48 hours if an individual's privileges to access education records has been withdrawn and the date withdrawal occurred.
    f. CONTRACTOR shall require and ensure annual training of those individuals determined to have access due to a legitimate educational interest in the education records. The training shall include the federal and state laws relating to student and family privacy and best practices for maintaining student and family privacy.
    g. CONTRACTOR shall maintain past and current lists of individuals attending training and the related training materials.
    h. CONTRACTOR shall not disclose the education records to individuals within CONTRACTOR who have not been determined to have a legitimate educational interest, who have not received training, and who have not signed a non-disclosure agreement.

8. CONTRACTOR shall only access, collect, store, process, or use the education records, as necessary to provide the services set forth in the Contract for its legitimate educational interest in the education records. Therefore, CONTRACTOR will not access, collect, store, process, sell, disclose, de-identify or use the education records for any other purpose.
9. Data disclosed by USBE to Contractor includes records that: (1) may directly relate to a student; (2) may contain personally identifiable information, and (3) are maintained by an educational agency or institution or by a party acting for the agency or institution. SPECIFICALLY, USBE shall provide the particular data which is described in ATTCH D of this contract. In addition to the identification and description of the data, Attachment D shall also contain a description of the frequency and method of secure file transfer. USBE has no obligation to provide data not described in ATTCH D.
10. CONTRACTOR shall not re-disclose the education records to any other party without the prior consent of the parent or eligible student.
11. CONTRACTOR shall protect all education records in a manner that does not permit disclosure of the educational records to anyone other than those individuals within its organization to whom CONTRACTOR has determined to have legitimate educational interests in the education records.
12. CONTRACTOR shall store and maintain all education records separately from the information of any other records.
13. CONTRACTOR shall notify the Board if there are any changes that will affect the system where all education records are stored and maintained, and ensure the system is in compliance with industry standards for the security and privacy of education records.
14. CONTRACTOR shall comply with all state and federal laws relating to student or family privacy and will maintain any and all education records in a manner consistent with such laws.
15. CONTRACTOR shall notify the Board in writing immediately upon discovering any breach, or suspected breach of security, or any disclosure of education records to an unauthorized individual within CONTRACTOR's organization, or re-disclosure to anyone. Notification shall include the date of improper release and a secure transmission of list(s) of affected students or families to assist the Board in notifying students, parents, or guardians of the improper release as required by federal and state law. CONTRACTOR agrees the improper release of any education record constitutes a material breach of the Contract. CONTRACTOR shall be liable for any claims or damages that occur from its failure to comply with its obligations in this Attachment.
16. CONTRACTOR shall return to the Board or securely destroy any education records and PII provided pursuant to the Contract upon the earlier of either the expiration or termination of the Contract.
17. Notices required by this Attachment shall be provided to:
    Chief Privacy Officer, who is currently Dr. Whitney Phillips at Whitney.Phillips@schools.utah.gov.

EAST HOLLYWOOD HIGH SCHOOL
Data Breach

A data breach is any instance in which there is an unauthorized release or access of PII or other information not suitable for public release. This definition applies regardless of whether an organization stores and manages its data directly or through a contractor, such as a cloud service provider. Data breaches can take many forms including

- hackers gaining access to data through a malicious attack;
- lost, stolen, or temporary misplaced equipment (e.g., laptops, mobile phones, portable
- thumb drives, etc.);
- employee negligence (e.g., leaving a password list in a publicly accessible location, technical
- staff misconfiguring a security service or device, etc.); and
- policy and/or system failure (e.g., a policy that doesn't require multiple overlapping security
- measures—if backup security measures are absent, failure of a single protective system can
- leave data vulnerable)

To prevent a data breach, EHHS shall prepare and maintain data privacy and security policies and procedures in accordance with industry best practices, and as required under Utah state law. Some key components to a strong policy might include:

- Implement appropriate technical, administrative and physical security safeguards
- Review your information system(s) and data and identify where PII and other sensitive information resides
- Continuously monitor for PII and other sensitive data leakage and loss
- Consider establishing relationships with outside advisors who are knowledgeable about data breaches (e.g., IT, forensics and counsel)
- Track data breach laws, rules and notification mandates
- Prepare and implement a data breach response policy and procedure
    - Assemble a data incident response team and applicable roles
    - Outline critical steps to take within the first 24 hours of a suspected breach
    - Train staff to identify and report suspected breaches
    - Conduct a practice data breach response scenario

If a breach occurs, EHHS has a policy in place for response. Utah law §53A-1-1405 further requires EHHS to notify adult students or parents/legal guardians in the event of a breach involving student data. The check-list provided in this guidance was adapted from guidance provided by the US Department of Education's Privacy Technical Assistance Center (ptac.ed.gov) and can be used as a model for how to respond to a breach.

Data Breach Response Best Practices Checklist

- Validate the data breach
    a. Confirm breach has ended and lock-down of systems (e.g., change passwords and encryption keys)
    b. Isolate and preserve compromised systems and data
- Assign an incident manager to be responsible for the investigation
- Assemble your Data Breach Response Team
    a. Suggested stakeholders, as appropriate: School and District leadership, Legal, IT Security, Information Technology, your appointed Student Data Manager, Human Resources, Internal Auditors, District Communications/Public Relations
- Investigate scope of breach to determine types of information compromised and number of affected individuals

- Decide how to investigate the data breach to ensure that the investigative evidence is appropriately handled and preserved
- Attempt to retrieve lost or otherwise compromised data
- Determine whether notification of affected individuals is appropriate and, if so, when and how to provide such notification
    a. Identify notification timeframes and requirements
    b. Develop and deliver notices to affected individuals and agencies in accordance with regulatory mandates and timeframes
- Determine whether to notify the authorities/law enforcement (situation dependent)
    a. Involve counsel to analyze legal obligations

Tips:

- Document your work, but coordinate with counsel on preparation and treatment of written materials related to the breach
- Act swiftly, as regulatory timeframes begin upon discovery of the breach
- Evaluate the need for a toll-free number for affected individuals to receive specific information and assistance
- Consider offering credit monitoring, identity repair services, or identity theft insurance for affected individuals
- Cooperate with regulatory and governmental inquiries

Sample Data Breach Letter Best Practices

DISTRICT LETTERHEAD

[PARENT OR LEGAL GUARDIAN NAME]

[STREET ADDRESS]

[CITY, STATE AND ZIP CODE]

[DATE]

Dear [PARENT OR LEGAL GUARDIAN NAME],

The first paragraph should reaffirm your school and district's commitment to data privacy. It should say that there has been a breach and that you are committed to protecting students, staff and their privacy.

What Happened?

Next, you should include a brief description of the data breach incident in general, and accessible terms. Avoid too much jargon or technical information that might leave you vulnerable again. Details should include the date of the breach or, if unknown, the approximate date or date range of the breach. You could describe whether data was hacked, mistakenly sent insecurely, if a computer or other device was forgotten or lost, or if there was a physical break-in or theft.

What information was involved?

Recipients will want to know what data was breached. If you know the data that was compromised, provide as much detail as possible without further compromising your security systems (see example letters for ideas).

What is [LEA NAME] doing in response?

Provide a brief description of the actions taken by the school or district to contain the breach and protect data from further unauthorized access or use. For example, did you require every user to change their password? Did you restore your gradebooks to the state they were prior to the breach? Did you verify the recipient deleted all copies of the inadvertent data sent to them?

If this notice was delayed because of law enforcement investigation, you should explain that so you can be clear about the timeline of your response.

What is [LEA NAME] doing to prevent this from happening in the future?

Here, recipients will want to know what steps you have implemented, or will implement, to prevent this type of breach. Of course, there is no way to anticipate all possible threats, but you can use this as an opportunity to reexamine your policies, procedures, training, and audit/review regarding data privacy. Analyze the root cause of the situation and identify where your vulnerabilities are.

What additional steps you can take?

Next, provide information on resources available to and advice on actions affected individuals should take. If the breach involves social security numbers or other potentially vulnerable PII, you should consider providing free credit monitoring for affected parties for 1 to 2 years and provide information on how to sign up for the service. If student educational records were compromised, remind parents or legal guardians how to review the educational record and their rights to correct anyerrors.

Where can you get more information on this issue?

Here, list all relevant contact information for the individual at the district who can answer questions, law enforcement or other government authorities and, as appropriate, contact information for national consumer reporting agencies.

Close by once again reaffirming your LEA's commitment to privacy and a great education.

Sincerely,

X_____

[LEA Name] [Superintendent or other relevant leader]

East Hollywood High School

Employee Data Sharing and Confidentiality Agreement

To minimize the risk of human error and misuse of information, East Hollywood High School will provide a range of training opportunities for all EHHS staff, including volunteers, contractors and temporary employees with access to student educational data or confidential educator records.

All EHHS employees and contracted partners must sign and obey the **Employee Acceptable Use Policy**, which describes the permissible uses of state technology and information. EHHS employees and contracted partners also must sign and obey the **Employee Data Sharing and Confidentiality Agreement**, which describes appropriate uses and the safeguarding of student and educator data. New EHHS employees must sign the aforementioned documents prior to being granted access to EHHS systems. As of the adoption of this policy, existing EHHS employees will be given 90 days to complete the required training and sign the aforementioned documents.

Thereafter, all employees will be required to participate in an annual **Data security and privacy fundamentals** training, which is mandatory for continued access to EHHS's network. These signed agreements will be maintained in the employee's file located in the Principal/Directors office. Non-compliance with the agreements shall result in consequences up to and including removal of access to EHHS network; if this access is required for employment, employees and contractors may be subject to dismissal.

Additionally, EHHS requires targeted information security and privacy training for specific groups within the agency and provides updated guidance to local education agencies concerning compliance with state and federal privacy laws and best practices in this ever-changing environment.

East Hollywood High School

Prohibited Activities without Prior Consent

In accordance with 53A-13-301 and 53A-13-302, LEAs shall adopt policies governing the protection of family and student privacy. These policies shall require prior written consent of the parent or legal guardian of a student before administering and collecting the information listed below, whether information is personally identifiable or not.

Prohibited Activities:

Any psychological or psychiatric examination, test, or treatment, or any survey, analysis, or evaluation, in which the purpose or intended effect is to cause the student to reveal information concerning the student's or any family member's:

(a) political affiliations or political philosophies;
(b) mental or psychological problems;
(c) sexual behavior, orientation, or attitudes;
(d) illegal, anti-social, self-incriminating, or demeaning behavior;
(e) critical appraisals of individuals with whom the student or family member has close family relationships;
(f) religious affiliations or beliefs;
(g) legally recognized privileged and analogous relationships, such as those with lawyers, medical personnel, or ministers; and
(h) income, except as required by law.

A general consent used to approve admission to school or involvement in special education, remedial education, or a school activity does not constitute written consent under this policy

Prior written consent shall be required from the parent or legal guardian of a student in all grades, kindergarten through grade 12

Prior written consent shall be required for activities within the curriculum as well as other school activities.

Requirements for Valid Prior, Written Consent:

Parent shall be provided written notice, at least two weeks prior to administration (except in response to a situation which a school employee reasonably believes to be an emergency, or as authorized under Title 62A, Chapter 4a, Part 4, Child Abuse or Neglect Reporting Requirements, or by order of a court). Following disclosure, a parent or guardian may waive the two-week minimum notification period.

This notice shall include:

1. Notice that a copy of the educational or student survey questions is made available at the school
2. An Internet address where a parent or legal guardian can view the exact survey to be administered
3. Reasonable opportunity to obtain written information concerning:

a. Records or information, including information about relationships, that may be examined or requested;
b. how the records or information shall be examined or reviewed;
c. how the information is to be obtained;
d. the purposes for which the records or information are needed;
e. the entities or persons, regardless of affiliation, who will have access to the personally identifiable information; and
f. a method by which a parent of a student can grant permission to access or examine the personally identifiable information.

Authorization:

The prior consent is valid only for the activity for which it was granted, unless otherwise agreed to by a student's parent or legal guardian and the person requesting written consent,

To terminate the authorization, the authorizing parent or guardian shall submit a written withdrawal of authorization to the school principal.

Exceptions:

If a school employee or agent believes that a situation exists which presents a serious threat to the well-being of a student, that employee or agent shall notify the student's parent or guardian without delay, unless the matter has been reported to the Division of Child and Family Services within the Department of Human Services.

If a school employee, agent, or school resource officer believes a student is at-risk of attempting suicide, physical self-harm, or harming others, the school employee, agent, or school resource officer may intervene and ask a student questions regarding the student's suicidal thoughts, physically self-harming behavior, or thoughts of harming others for the purposes of:

1. Referring the student to appropriate prevention services
2. Informing the student's parent or legal guardian

In accordance with §53A-11a-203(3), schools shall notify parents or legal guardians of such threats and incidents. Following parent notification of student suicide threat, bullying incident, cyber-bullying incident, harassment incident, hazing incident or retaliation incident, schools shall maintain a record of the notification, securely and confidentially, consistent with §53A-11a-203.

A sample record of parental notification is provided in Appendix XYZ

East Hollywood High School

RECORD OF PARENT NOTIFICATION OF STUDENT THREAT OR INCIDENT
Required by 53A-11a-203
[H.B. 134, 2013 Legislative Session]

This form is a record required to be maintained securely and confidentially by the school consistent with §53A-11a-203(3) following parent notification of student suicide threat, bullying incident, cyber-bullying incident, harassment incident, hazing incident or retaliation incident. THIS FORM SHOULD NOT BE USED TO NOTIFY PARENT(S) OF THE INCIDENT.

Student's name: _____

Parent(s) name: _____

Date of incident: _____

Parent was notified of the incident by:

_____ _____
Designated School Employee's Name Signature

On _____by ___phone ___email ___mail ___other
Date

Provide parent contact information:

_____

_____

Parent was notified of:

____suicide threat
_____bullying incident
_____cyber-bullying incident
_____harassmentincident
_____hazing incident
_____retaliation incident

East Hollywood High School
Record Retention and Expungement

Board Rule- Record retention and expungement

East Hollywood High will retain and dispose of student records in accordance with Section 63G-2-604, **53A-1-1407**, and comply with active retention schedules for student records per Utah Division of Archive and Record Services.

In accordance with **53A-1-1407**, EHHS shall expunge stored student data upon request of a student who is at least 23 years old. EHHS may expunge medical records and behavioral test assessments. EHHS shall not expunge student records of grades, transcripts, and a record of the student's enrollment or assessment information.

EHHS may create and maintain a cumulative disciplinary record for a student.

East Hollywood High School
Acceptable Use Policy for Internet and Network Access

The goal of using the Internet is to provide support for the public education system. The Internet is a world-class tool for educators, students, and parents. It can provide many exciting educational resources and learning opportunities. Unfortunately, there are materials on the Internet that are controversial in nature that do nothing to promote the educational process. It is important that all who access the Internet demonstrate judgment on the information that they access. The following is prohibited:

1. Any use of the Internet for illegal or inappropriate purposes to access materials that are objectionable in a public school environment. Inappropriate use is defined as use in violation of the intended use of the Internet, to provide information to support the educational process. (e.g., Instant Messenger, chat rooms, steaming video, audio, Internet radio, file sharing, MP3 downloading, and burning copies of copyrighted CDs are prohibited).
2. Any use for commercial purposes, financial gain or political lobbying.
3. Access to the Internet without parental permission.
4. Any unauthorized use of the FFCHS network.

It is understood that East Hollywood High School, the Utah State Office of Education, and the Utah Education Network have no control of the information on the Internet. Some sites on the Internet may contain material that is illegal, defamatory, inaccurate, or potentially offensive to some people. While the student will receive supervision and guidance while using the Internet, it is his/her responsibility to choose not to access materials that do not fit the goal of Internet use at EHHS.

Students that break this Acceptable Use Policy may face one or all of the following consequences:

1. Loss of network / Internet access
2. Removal from class (timeout or conference)
3. Parent conference
4. Suspension from school for the remainder of the term
5. Expulsion from school for repeated violation
6. Civil and criminal charges filed against the student

I have read the Student Contract and the Internet Acceptable Use Policy and agree to all terms therein.

_____ _____
Student Signature Date

I give permission for the student who has signed the above statement to have access to the Internet at Fast Forward Charter High School.

_____ _____
Parent/Guardian Signature Date