CENTER FOR CREATIVITY, INNOVATION, AND DISCOVERY

Student Data Privacy and Security Governance Policy and Plan

Statement of Purpose

The Board of Directors of the Center for Creativity, Innovation, and Discovery (CCID) affirms that the efficient collection, analysis, and storage of student information are essential to improve the education of students. CCID recognizes the need to exercise care in the handling of confidential student information.

CCID also recognizes that the privacy of students and the use of confidential student information are protected by federal and state laws, including the Family Educational Rights and Privacy Act (FERPA), Utah Code §53E-9-3, Student Privacy and Data Protection, and Utah Admin. Code R277-487, Public School Data Confidentiality and Disclosure. CCID acknowledges that violation of federal or state law, or Utah State Board of Education (USBE) rule may result in civil penalties.

Data Maintenance and Protection Policy

CCID recognizes that there is risk and liability in maintaining student data and other education-related data. The school will, therefore, incorporate reasonable data industry best practices to mitigate this risk in accordance with law. The policy is designed to ensure only authorized disclosure of confidential information.

The governance plan provides an organizational approach to the acquisition, use, security, and disposal of education data in order to protect student privacy. The Board of Directors has designated the Executive Director and the Director of Educational Technology as the Student Data Privacy Managers at CCID.

Compliance Process

In accordance with Utah Admin. Code R277-487, the school will meet the following compliance measures:

- Designate an individual as an Information Security Officer;
- Adopt the CIS Controls or comparable;
- Report to the USBE by October 1st of each year regarding the status of the adoption of the CIS controls, or comparable, and future plans for improvement.

Governing Principles

This governance plan incorporates the following Generally Accepted Information Principles (GAIP):

- Risk**:** There is risk associated with data and content. The risk must be formally recognized, either as a liability or through incurring costs to manage and reduce the inherent risk.
- Due Diligence**:** If a risk is known, it must be reported. If a risk is possible, it must be confirmed.
- Audit**:** The accuracy of data and content is subject to periodic audit by an independent body.
- Accountability**:** An organization must identify parties which are ultimately responsible for data and content assets.
- Liability**:** The risk in information means there is a financial liability inherent in all data or content that is based on regulatory and ethical misuse or mismanagement.

Definitions

Administrative Security: consists of policies, procedures, and personnel controls including security policies, training, audits, technical training, supervision, separation of duties, rotation of duties, recruiting and termination procedures, user access control, background checks, performance evaluations, disaster recovery, contingency, and emergency plans. These measures ensure that authorized users know and understand how to properly use the system in order to maintain security of data.

Aggregate Data: is collected or reported at a group, cohort, or institutional level and does not contain Personally Identifiable Information (PII).

Data Breach: is the unauthorized acquisition of PII.

Logical Security: consists of software safeguards for an organization's systems, including user identification and password access, authenticating, access rights, and authority levels. These measures ensure that only authorized users are able to perform actions or access information in a network or a workstation.

Personally Identifiable Information (PII): includes: a student's name; the name of the student's family; the student's address; the student's social security number; a student education unique identification number or biometric record; or other indirect identifiers such as a student's date of birth, place of birth, or mother's maiden name; and 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.

Physical Security: describes security measures designed to deny unauthorized access to facilities or equipment.

Significant Data Breach: means a data breach where an intentional data breach successfully compromises student records; a large number of student records are compromised; sensitive records are compromised, regardless of number; or a breach of data that an LEA deems to be significant based on the surrounding circumstances.

Student Data: means data collected at the student level and included in a student's educational records.
Unauthorized Data Disclosure: is the intentional or unintentional release of PII to an unauthorized person or untrusted environment.

Data Collection
CCID follows applicable state and federal laws related to student privacy in the collection of student data.

Data Supervisory Officers
Executive Director as LEA Data Manager
The Executive Director has the following data management responsibilities:

- To authorize and manage the external sharing of PII from a cumulative record;
- To share personally identifiable student data under the following circumstances:
    - Of a student with the student and the student's parent;
    - When required by State or Federal law;
    - In an aggregate form with appropriate data redaction techniques applied;
    - For a school official;
    - For an authorized caseworker or other representative of the Department of Human Services or the Juvenile Court;
    - In response to a subpoena issued by a court;
    - As directory information;
    - In response to submitted data requests from external researchers or evaluators.
    - To ensure that personally identifiable student data is not shared for the purpose of external research or evaluation;
    - To create and maintain a list of all school staff that have access to personally identifiable student data;
    - To provide annual school-level training on data privacy to all staff members, including volunteers.

Director of Educational Technology
The Director of Educational Technology has the following data management responsibilities:

- To act as the primary local point of contact for the state student data officer;
- To act as the officer supporting the Executive Director in administering oversight of student data;
- To ensure compliance with security systems laws throughout the school's system, including:

    - Providing training and support to applicable employees; and,
    - Producing resource materials and plans for school data security.
- To investigate complaints of alleged violations of systems breaches;
- To provide an annual report to the Board of Directors on the school's systems security needs.

Access to Personally Identifiable Information (PPI)

- Unless prohibited by law or court order, the school provides parents, legal guardians, or eligible students, as applicable, the ability to review their child's educational records and student performance data per state and federal law;
- The school allows for authorized purposes, uses, and disclosures of data maintained by the school as a Local Education Agency (LEA);
- The Executive Director grants, removes, and reviews user access to student data.
- The school makes public information about student data privacy and security safeguards that protect the school's data from unauthorized access and use;
- The school provides contact information and a process for parents and students to request student and public-school information from CCID consistent with the law;
- The board's Audit Committee conducts an annual review of existing access and security safeguards;
- Access to PII maintained by the school shall be restricted to: (1) authorized staff who require access to perform their assigned duties; and (2) authorized employees of the USBE who require access to perform their assigned duties; and (3) vendors who require access to perform their assigned duties.
- The school's Student Data Privacy Manager may not share PII outside of the school as an educational entity without a data authorization except:
    - With the student and the student's parent;
    - With a school official;
    - With an authorized caseworker or other representative of the Department of Human Services or Utah Juvenile Court, Division of Juvenile Justice Services, Division of Child and Family Services, Division of Services for People with Disabilities;
    - In response to a subpoena issued by a court, but not outside of the use described in the subpoena; and,
    - With a person to whom the Student Data Privacy Manager's education entity has outsourced a service or function to research the effectiveness of a program's implementation or to perform a function that the education entity's employees would typically perform.

- The Student Data Privacy Manager may not share PII for the purpose of external research or evaluation.

Security
The school has in place administrative security, physical security, and logistical security controls to protect from a data breach or from an unauthorized data disclosure that generally follow best practices for hard copy records and the cybersecurity framework developed by the Center for Internet Security. In any significant disclosure of student data, the school will take the following steps:

- Notify the USBE and the school's authorizer within ten 910) working days in the case of a confirmed, unauthorized, significant disclosure of student data either by the school or by third parties;
- Notify in a timely manner any affected individuals, students, and families if there is a confirmed data breach or a confirmed unauthorized data disclosure;
- Notify the student, if the student is an adult student, or notify the student's parent or legal guardian, if the student is not an adult student, if there is a release of a student's PII due to a security breach;

Acknowledgement of Prohibition on Selling Data
In accordance with Utah Admin. Code R277-487, CCID acknowledges that data maintained by the school, including data provided by contractors, may not be sold or used for marketing purposes, except with regard to authorized uses or directory information not obtained through a contract with an educational agency or institution.

Employee Non-Disclosure Assurances
All CCID board members, employees, contractors, and volunteers must sign and obey the acknowledgements and agreements which describe the permissible uses of student data, state technology, and information maintained by the school; the privacy and confidentiality of student data, even after a board member, employee, contractor, or volunteer is no longer affiliated with the school; and prohibitions and limitations regarding access to PPI and student records.

Non-compliance with non-disclosure and confidentiality agreements shall result in consequences up to and including removal of access to the school's network and possible dismissal.

Data Disclosure Protocols
This policy establishes the protocols and procedures for sharing data maintained by the school consistent with the Family Educational Rights and Privacy Act (FERPA), Utah

Code §53E-9-3, Student Privacy and Data Protection, and Utah Admin. Code R277-487, Public School Data Confidentiality and Disclosure.

- The school will provide parents with access to their child's educational records, or an eligible student access to his or her own educational records, within 45 days of receiving an official request.
- The school is not required to and will not provide information to parents or an eligible student concerning another student, the financial records of parents, and confidential letters of recommendation if the student has waived the right to access.
- The school is not required to provide data that it does not maintain; nor is the school required to create education records in response to an eligible student's request.
- Publicly released reports shall not include PII and shall use aggregate data in such a manner that re-identification of individual students is not possible.
- The school will clearly define in its registration materials what data is determined to be directory information.
- The school will notify parents in writing at registration about directory information, which includes PII, and offer parents an opportunity to opt out of the directory. If a parent does not opt out, the release of the information as part of the directory is not a data breach nor an unauthorized data disclosure.
- The school will annually train employees, aides, and volunteers regarding confidentiality of personally identifiable student information and student performance data.
- The school provides a disclosure statement to parents or guardians of students that meets the following criteria:
    - Is a prominent, stand-alone document;
    - Is annually updated and published on the school's website;
    - States the necessary and optional student data collected by the school;
    - States that the school will not collect student data prohibited by Utah Code §53E-9-3, Student Privacy and Data Protection;
    - States that the school will not share legally collectible data without authorization;
    - States that students and parents are responsible for the collection, use, or sharing of student data as described in Utah Code §53E-9-304 which states that a student owns their personally identifiable student data; and that a student may download, export, transfer, save, or maintain the student's data, including documents;
    - Describes how the school may collect, use, and share student data;

    - Includes the following statements: “The collection, use, and sharing of student data has both benefits and risks. Parents and students should learn about these benefits and risks and make choices regarding student data accordingly.”
    - Describes in general terms how the school stores and protects student data; and,
    - States a student’s rights related to their data.

Required Employee Actions to Protect Student Data
All school employees must take the following actions routinely in order to protect student data:

- Complete student data privacy and security training;
- Consult with school internal data officers when creating or disseminating reports containing data;
- Use password-protected computers/devices when accessing any student-level or staff-level records;
- Refuse to share individual passwords for personal computers or data systems with anyone without authorized access;
- Log out of any data system/portal and close the browser after each use;
- Store sensitive data on appropriate, secured location;
- Keep printed reports with PII in a locked location while unattended;
- Use a secure document destruction service provided at the school when disposing of records containing PII;
- Refuse to share personally identifying data during public presentations, webinars, etc., if users need to demonstrate child/staff level data;
- Redact any PII information when sharing sample reports with general audiences in accordance with guidance provided by the student data manager;
- Take steps to avoid disclosure of PII in reports, such as aggregating, data suppression, rounding, recording, blurring, perturbation, etc.;
- Delete files containing sensitive data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties;
- Do not use email to send screenshots, text, or attachments that contain PII or other sensitive information. If users receive an email containing such information, they must 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;
- Use school-approved, secure methods when sharing or transmitting sensitive data;

- Share within secured server folders appropriate for the school's internal file transfer;
- Do not transmit child/staff-level data externally unless expressly authorized in writing by the data owner, and then only transmit data via approved methods;
- Limit use of individual data to the purposes which have been authorized within the scope of an employee's job responsibilities.

Data Disclosure to Requesting External Person or Organizations

The school 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 requirements, audit, or evaluation, and then only within parameters allowed by law.

- A requesting governmental agency must provide evidence of the federal or state requirements to share data in order to satisfy FERPA disclosure exceptions.
- The Director of Educational Technology will ensure that the proper data disclosure avoidances are included if necessary.

The school may share data that do not disclose personally identifiable information with an external researcher or evaluator for projects unrelated to federal or state requirements if the following conditions have been met:

- A school director or board members sponsors an external researcher or evaluator request;
- Student data are not PII and are de-identified through disclosure avoidance techniques and other pertinent techniques as determined collaboratively by the Executive Director and the Director of Educational Technology;
- Researchers and evaluators provide a copy of any publication or presentation to the school that uses the school's data at least 10 days prior to any publication or presentation.

Training and Support Policy

CCID recognizes that training and supporting teachers and staff regarding federal and state data privacy laws is a necessary control to ensure legal compliance. The school administration and data managers will ensure that the following trainings occur:

- Educators who have access to student records will receive an annual training on confidentiality of student data. The content of this training will be based on this policy.
- By October 1st each year, the data manager will report to the USBE the completion status of the annual confidentiality training and provide a copy of the training materials used.

- The data manager shall keep a list of all employees who are authorized to access student education records after having completed a training that meets the requirements of Utah Code §53E-9-204.
- The administration will also train volunteers with authorized access to student educational data or confidential educator records in order to minimize the risk of human error and misuse of information.
- The school will require all employees and volunteers to sign agreements and assurances, as well as responsible technology use agreements, which describe the permissible uses of technology and information, and which prohibit employees from disclosing confidential, personally identifiable information.
- The school will provide targeted security and privacy training for data stewards and IT staff, as well as for any other groups that collect, store, or disclose data at the school.
- Participation in the training will be required and documented.

Third Party Vendors

The school's contracts with outside vendors involving student data, which govern databases, online services, assessments, special education or instructional supports, shall include the following provisions which are intended to safeguard student privacy and the security of the data:

- Require that the third-party provider meet the definition of a school official under 34 CFR 99.31 (a)(1)(i)(B); this definition allows for the inclusion of 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;
- Require that the third-party provider assure compliance with), Utah Code §53E-9-3, Student Privacy and Data Protection, and Utah Admin. Code R277-487 through its MOU with the school;
- Require that the contract between the school and the third-party provider include a provision that the data is the property of the school;
- Require that the vendor agree to comply with any and all applicable state and federal law;
- Require that the provider have in place administrative security, physical security, and logistical security controls to protect from a data breach or unauthorized data disclosure;
- Require that the provider restrict access to PII to the authorized staff or only to those providers who require such access to perform their assigned duties;
- Prohibit the provider's secondary use of PII, including for use in sales, marketing or advertising;

- Require that the school monitor and maintain control of the data;
- Require that, if the school's contract with a third-party provider allows collection and access to the school's data, the school must notify a student and the student's parent or guardian in writing that the student's data is collected and maintained by the third-party provider;
- Require that data be destroyed within an associated timeframe; and.
- Provide penalties for non-compliance with the above provisions.
- Ensure that third-party contractors are aware that they are legally allowed to engage in the following activities:
    - Using student data for adaptive learning or customized student learning purposes;
    - Marketing of an educational application or product to a parent or legal guardian of a student, if the third-party contractor did not use student data, shared by or collected on behalf of school to market the educational application or product;
    - Using a recommendation engine to recommend services or content that relates to learning or employment within the third-party contractor's internal application, if the recommendation is not motivated by payment or other consideration from another party;
    - Responding to a student's request for information or feedback, if the content of the response is not motivated by payment or other consideration from another party;
    - Using student data to allow or improve the operability and functionality of the third-party contractor's internal application.

Return of Data by Third-Party Vendors

At the completion of a contract with the school, if the contract has not been renewed, a third-party contractor will return all personally identifiable student data to the school; and to the maximum extent possible, the third-party vendor will delete all personally identifiable student data related to the third-party contractor's work.

Prohibitions for Third-Party Vendors

Prohibitions

In accordance with Utah Code §53E-9-309, a third-party contractor may not sell student data; may not collect, use, or share student data, if the collection, use, or sharing of the student data is inconsistent with the third-party contractor's contract with the school; and may not use student data for targeted advertising.

Notwithstanding the above prohibitions, a third-party vendor may obtain student data through the purchase of, merger with, or otherwise acquiring of a third-party contractor if

the third-party contractor remains in compliance with state and federal law, this board policy, and the school's previous contract with the original third party.

Limitations

The provisions of this section of the Governance Policy and Plan do not apply to the use of an external application, including the access of an external application with login credentials created by a third-party contractor's internal application; nor do they apply to the providing of internet service; nor do they impose a duty on a provider of an interactive computer service, as defined by Utah Code §53E-9-3, Student Privacy and Data Protection.

Expungement Request Procedures

The school recognizes the risk associated with data following a student year after year that could be used to mistreat the student. Some records may not be expunged even at the request of a parent or an adult student. These include grades, transcripts, a record of the student's enrollment, and assessment information.

The school will consider all other requests for expungement of records based on the amendment procedure found in 34 CFR 99, Subpart C of FERPA as listed below:

- If a parent or adult student believes that a record is misleading, inaccurate, or in violation of the student's privacy, they may request that the record be expunged.
- The school will decide whether to expunge the data within a reasonable time after the request.
- If the school decides not to expunge the record, the school will inform the parent or an adult student of the decision, as well as the right to an appeal hearing.
- The school shall hold a hearing within a reasonable time after receiving the request for a hearing.
- The school shall provide the parent or adult student with notice of the date, time, and place in advance of the hearing.
- The hearing shall be conducted by any individual at the school that does not have a direct interest in the outcome of the hearing.
- The school shall give the parent or an adult student a full and fair opportunity to present relevant evidence. At the expense and choice of the parent or adult student, the parent or adult student may be represented by an individual of their choice, including an attorney.
- The school shall make its decision in writing within a reasonable time following the hearing.
- The decision must be based exclusively on evidence presented at the hearing and include a summary of the evidence and reasons for the decision.

- If the decision is to expunge the record, the school will seal it or make it otherwise unavailable to other staff and educators.

Quality Assurances and Transparency Requirements

The quality of data is a function of accuracy, completeness, relevance, consistency, reliability, appropriate accessibility, and data interpretation and use. This policy is structured to encourage the effective and appropriate use of educational data. The school acknowledges that adherence to compliance and data-driven decision-making guide what data is collected, reported, and analyzed at the school.

- Where possible, data are collected at the lowest level available (at the student/teacher level); no aggregate data collections are necessary if the aggregate data can be derived or calculated from the detailed data.
- For all data collections, the school establishes clear guidelines for data collection and the purpose of the data request.
- The school's state-level data are audited by external, independent auditors yearly as a check on accuracy or to investigate the source of any anomalies.
- Before releasing high-risk data, the Executive Director and Director of Educational Technology must complete a review of the reliability, validity, and presentation of the data, and must follow all protocols in this policy related to appropriate disclosure.

Data Transparency and Sharing Procedures

CCID acknowledges that there is a risk of redisclosure whenever student data are shared. The school shall follow appropriate controls to mitigate the risk of redisclosure and to ensure compliance with federal and state law:

- A data manager shall approve all data sharing or designate other individuals who have been trained on compliance requirements with FERPA.
- A data manager shall oversee the school's procedures for approving websites.
- Teachers and staff are authorized to share student information only to administrators, school counselors, teachers, staff members, school medical professionals, and other school officials who need this information in order to serve the educational needs of the child.
- Teachers and staff may also share student information with a specific student's parents or guardians.
- Communications between students and teachers, teachers and parents, or students and other students that may be collected or held by a third-party educational technology vendor must have prior approval of the school's data manager and are subject to all the requirements of this policy related to PII and third-party vendors.

- Teachers must utilize only those applications or services approved by the school's data managers.
- Teachers must reference the school's approved list of educational, technology products, services, websites, applications before using such tools.
- Teachers are ethically obligated to follow and model good digital citizenship practices and behaviors with their students. This obligation includes thinking carefully about the digital processes incorporated into any project, lesson, or pedagogical tool.
- In accordance with the), Utah Code §53E-9-3, Student Privacy and Data Protection, and Utah Admin. Code R277-487, Public School Data Confidentiality and Disclosure, the school will annually publish all its disclosures of student personally identifiable information on the Metadata Dictionary site on Data Gateway. The school will also provide a link from its website to the Metadata Dictionary where this disclosure may be found.
- After sharing from student records, the data manager shall make a note in the student record of the exchange in accordance with 34 CFR 99.32 (FERPA).
- For external research, the data manager shall ensure that the study follows the requirements of FERPA's study exception described in 34 CFR 99.31(a)(6).
- The Board of Directors must approve any extensive research requests.

Data Breach Protocols

In the event of a data breach or inadvertent disclosure of personally identifiable information (PII), CCID staff shall follow industry best practices, state and federal laws, as well as administrative rules in responding to the breach. The school's data breach protocols are listed below:

- Identify the Data Breach: Determine whether a data breach has occurred or not. Identifying a data breach includes searching for leads and/or security vulnerabilities within the school's network, a security breach that affects the general network, an attack by a cyber attacker group, or other breaches. An indicator specifies that a breach has been experienced or is in action. The school will also identify all affected data, machines, and devices.
- Internal Reporting of Data Breach: Concerns about security breaches must be reported immediately to the Executive Director or Director of Educational Technology who will collaborate with appropriate school administrators to determine whether a security breach has occurred.
- Assign an Incident Manager. Once a breach has been validated, the school will immediately assign an incident manager to be responsible for the investigation, documentation, and the reporting process. The incident manager will also

coordinate the flow of information and manage public messages about the breach.

- Create a Response Team. The school will assemble an incident response team to take the following actions:
    - Determine the status and scope of the breach (on-going, active, or post breach);
    - If the breach is active or on-going, take actions to prevent further data loss by securing and blocking unauthorized access to systems/data;
    - Preserve evidence for investigation;
    - Document all mitigation efforts for later analysis;
    - Advise staff who are informed of the breach to keep breach details in confidence until notified otherwise.
- Take Emergency Intervention Precautions: When a data breach or possible data breach has been identified, record the date and time the data breach was identified. The individual who identified the data breach must quickly report to the internal responsible parties. Then an access restriction should be imposed on the data in order to prevent dissemination of critical data that was leaked. Other emergency intervention precautions include collecting all possible data regarding the leak, meeting with the individuals who recognized the data breach, and doing a risk assessment.
- Preserve Evidence. When possible, the school will preserve evidence (backups, images, hardware, etc.) for later forensic examination. The school will locate, obtain, and preserve all written and electronic logs and records applicable to the breach for examination whenever possible.
- Analyze the Data Breach: After gathering data regarding the breach, analyze the data. A review could include suspicious traffic, privileged access, duration of the threat, software and individuals involved in the breach, and the type of breach (internal or external). The school will conduct interviews with key personnel and document facts. If criminal activity is suspected, the school will coordinate these interviews with law enforcement.
- Appropriately Handle Breach Response Documentation: The school will collect and review any breach response documentation and analyze reports in the following manner:
    - Assess the data breach to determine the probable cause(s) and minimize the risk of future occurrence;
    - Address and/or mitigate the cause(s) of the data breach;
    - Solicit feedback from the responders and any affected entities;
    - Review breach response activities and feedback from involved parties to determine response effectiveness;

    - Make necessary modifications to the breach response strategy to improve the response process;
    - Enhance and modify information security and training programs, which includes developing countermeasures to mitigate and remediate previous breaches;
    - Integrate lessons learned so that past breaches do not reoccur.
- Restriction, Destruction, and Recovery Precautions: Restriction includes restricting access to the servers that were breached and also prevention of destruction of evidence to be used in the investigation. Destruction indicates destruction of all aspects that caused a breach; recovery indicates recovering the breached servers to their former states.
- Notification of Stakeholders: The school will notify all stakeholders affected by the breach as well as law enforcement. These stakeholders may include employees, families, adult students, business partners, and regulation authorities such as the USBE and the school's authorizer. This notification shall occur within 72 hours of the identified breach. If criminal activity is suspected, the school will notify law enforcement and follow any applicable federal, state, or local law relating to notification of law enforcement or other authorities.
- Focus on Post-Breach Operations: After taking the required precautions against the data breach, the incident manager and administration will review the school's cyber security network in detail, and create protocols and systems to prevent similar incidents in the future.

Additional Notification Procedures

CCID will take the following actions related to notifying data owners:

- Notify affected individuals whose sensitive information, including PII, has been compromised, as required by law;
- Provide notification in a straightforward and honest manner; avoid evasive or incomplete notifications;
- Foster a cooperative relationship between the incident response team and data owners;
- Work collaboratively with data owners to secure sensitive data, mitigate the damage that may arise from the breach, and determine the root cause(s) of the breach to devise mitigating strategies and prevent future occurrences;
- If the breach represents a threat to affected individuals' identity security, consider providing monitoring or protection services to mitigate the risk of negative consequences for those affected;
- Make every attempt to avoid news of the breach reaching the media before you notify affected individuals;

- Ensure that communication about the data breach comes from a collaborative effort between the Board of Directors and the administration regarding media notification, mailings, emails, phone calls, and in-person meetings;

Additional Procedures Related to Data Breaches

- Family Policy Compliance Office: The school may choose to notify the FPCO to seek technical assistance in the event of a data breach. Although FERPA does not require FPCO notification, the United States Department of Education considers it a best practice.
- Federal Privacy Council: The school may ask FPC to assist by helping to determine the potential for harm resulting from the release of the information; and to assist with FERPA compliance;
- Privacy Technical Assistance Center: The school may enlist PTAC to assist in providing the school with practical solutions for responding to privacy and security incidents, notification, and data recovery; assisting technical staff in conducting investigation and fact-finding activities; and helping school decision-makers with developing a strategy for incident mitigation and data recovery.
- Communication Protocol: The school will designate a single organizational representative, such as the Board Chair, the Executive Director, or the Incident Manager to initiate and/or communicate breach details to any party, including law enforcement.
- Advice from Legal Counsel: The school will regularly seek advice from legal counsel on the approved methods for protecting digital evidence to ensure that the school is prepared and able to properly preserve and document all evidence so that it can be used in a court of law, if necessary. This requires detailed recording and following proper collection, handling, storage, custody documentation, and destruction procedures.
- Collaboration with Law Enforcement: If applicable, the school will collaborate with law enforcement to ensure that in-house investigations do not interfere with law enforcement activities.
- Post-Breach Storage and Destruction of Data: Once investigative activities have been completed, the school will safely store, record, and, if applicable, destroy all evidence.
- Ensuring Proper Security Level of Resources and Devices: The school will consider all alternatives to replacing or clearing compromised resources and machines, including the cost of remediation or rebuilding of the assets to an acceptable security level.

Regular Updating of Data Security Protocols

The school will periodically update its data security protocols and resources in preparing for and responding to security breaches.

Policy Compliance

Failure to Comply

If the administration determines that one or more employees or contracted partners have substantially failed to comply with this policy and other relevant privacy policies, the team will determine appropriate consequences, which may include termination of employment or a contract and further legal action.

Concerns about Administrators Involved in Data Breaches

Concerns about security breaches that involve the Director of Educational Technology must be reported directly to the Executive Director. Concerns about security breaches that involve the Executive Director must be reported directly to the Chair of the Board of Directors.

Reviewed: December 5, 2024