EA Policy 3A.06.013 Student Data Privacy and Security Governance Policy

Statement of Purpose

Excelsior Academy affirms that the efficient collection, analysis, and storage of student information are essential to improve the education of our students. Excelsior Academy recognizes the need to exercise care in the handling of confidential student information as the use of student data has increased and as technology has advanced. Excelsior Academy also acknowledges that the privacy of students and the use of confidential student information is protected by federal and state laws, including the Family Educational Rights and Privacy Act (FERPA), the Utah Student Data Protection Act ("SDPA"), and the Utah Student Privacy Act ("SPA"). Excelsior Academy acknowledges that violation of the Utah SDPA and SPA may result in civil penalties.

Excelsior Academy's *Student Data Privacy and Security Governance Plan* has been adopted in accordance with the SDPA, U.C.A. §§53A-1-1401 and the Utah SPA. The plan 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. Excelsior Academy's Executive Director will designate the Student Data Privacy Manager.

Defined Terms

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.

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.

Collection

Excelsior Academy follows applicable state and federal laws related to student privacy in the collection of student data.

Data Supervisory Officers

Student Data Privacy Manager

The Student Data Privacy Manager has the following data management responsibilities:

- To authorize and manage the sharing outside the school 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 Excelsior Academy staff that have access to personally identifiable student data
- To ensure annual Excelsior Academy-level training on data privacy to all staff members, including volunteers
- Act as the primary local point of contact for the state student data officer
- Ensure compliance with security systems laws throughout the Excelsior Academy system, including:
    - Providing training and support to applicable Excelsior Academy employees, and,
    - Producing resource materials and plans for Excelsior Academy data security
- Investigate complaints of alleged violations of systems breaches
- Provide an annual report to the Board of Trustees on Excelsior Academy's systems security needs

Access to Personally Identifiable Information

- Unless prohibited by law or court order, Excelsior Academy provides parents, legal guardians, or eligible students, as applicable, the ability to review their child's educational records and student performance data as per state and federal law;
- Excelsior Academy allows for authorized purposes, uses, and disclosures of data maintained by Excelsior Academy as a Local Education Agency (LEA);
- The Executive Director is responsible for granting, removing, and reviewing user access to student data.

- Excelsior Academy allows parents, students, and the public access to information about student data privacy and the security safeguards that protect the data from unauthorized access and use;
- Excelsior Academy provides contact information and a process for parents and students to request student and public school information from Excelsior Academy consistent with the law;
- Excelsior Academy's Audit Committee conducts an annual review of existing access and security safeguards;
- Access to PII maintained by Excelsior Academy shall be restricted to: (1) the authorized staff of Excelsior Academy who require access to perform their assigned duties; and (2) authorized employees of the Utah State Board of Education who require access to perform their assigned duties; and (3) vendors who require access to perform their assigned duties and who have signed agreements to protect and secure such data.
- Excelsior Academy's Student Data Privacy Manager may not share PII outside of the school as an education 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

- Excelsior Academy has in place administrative security, physical security, and logical security controls to protect from a data breach or an unauthorized data disclosure.
- Excelsior Academy shall immediately notify the State Charter Director and the State Superintendent of Public Instruction in the case of a confirmed data breach or a confirmed unauthorized data disclosure.
- Excelsior Academy shall also notify in a timely manner affected individuals, students, and families if there is a confirmed data breach or a confirmed unauthorized data disclosure.
- If there is a release of a student's PII due to a security breach, Excelsior Academy shall notify the student, if the student is an adult student. If the student is not an adult student, Excelsior Academy will notify the student's parent or legal guardian.
- In accordance with R277-487-6, Excelsior Academy acknowledges that data maintained by Excelsior Academy, 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 Excelsior Academy board members, employees, contractors, and volunteers must sign and obey the Excelsior *Academy Employee and Volunteer Non-Disclosure Agreement* which describes the permissible uses of state technology and information.

Non-Compliance

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

Data Disclosure Protocols

This plan establishes the protocols and procedures for sharing data maintained by Excelsior Academy consistent with the disclosure provisions of the Federal Family Educational Rights and Privacy Act (FERPA) and Utah's SDPA.

- Excelsior Academy 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.
- Excelsior Academy 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.
- Excelsior Academy is not required to provide data that it does not maintain, nor is Excelsior Academy 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.
- Excelsior Academy has clearly defined in its communication plan and in registration materials for parents what data is determined to be directory information.
- Excelsior Academy notifies parents in writing at registration about directory information which includes PII and offers 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 or an unauthorized data disclosure.
- Excelsior Academy provides a disclosure statement to parents or guardians of Excelsior Academy students that meets the following criteria:
    - A prominent, stand-alone document;
    - Annually updated and published on Excelsior Academy's website;
    - States the necessary and optional student data that Excelsior Academy collects;
    - States that Excelsior Academy will not collect student data prohibited by the Utah Student Data Protection Act;
    - States that Excelsior Academy 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 Section 53A-1-1405 which states that a student owns his/her personally identifiable student data and that a student may

download, export, transfer, save, or maintain the student's data, including documents;
    - Describes how Excelsior Academy 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 Excelsior Academy stores and protects student data; and
    - States a student's rights related to his/her data.
- Excelsior Academy will train employees, aides, and volunteers regarding confidentiality of personally identifiable student information and student performance data, as defined in FERPA.

Data Disclosure to Requesting External Person or Organizations

- Excelsior Academy 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.
- 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.
- Excelsior Academy 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:
    - An Excelsior Academy Director or board member 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 Student Data Privacy Manager.
    - Researchers and evaluators supply Excelsior Academy a copy of any publication or presentation that uses Excelsior Academy data at least 10 days prior to any publication or presentation.

Data Security and Privacy Training

- Excelsior Academy will provide a range of training opportunities for all Excelsior Academy staff, including 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.
- Excelsior Academy will also require all employees and volunteers to sign both the *Network Access Policy and Agreement*, which describes the permissible uses of technology and information, and Excelsior Academy's *Confidentiality Agreement*, which prohibits employees' disclosure of confidential personally identifiable information.
- Excelsior Academy will also 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.
- Participation in the training is required and documented.

Third Party Vendors

- Excelsior Academy'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:
    - Requirement 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.
    - Requirement that the third-party provider assure compliance with Utah's SDPA through its MOU with Excelsior Academy;
    - Requirement that the contract between the LEA and the third party provider include a provision that the data is the property of Excelsior Academy;
    - Requirement that the vendor agree to comply with any and all applicable state and federal law;
    - Requirement that the provider have in place administrative security, physical security, and logical security controls to protect from a data breach or unauthorized data disclosure;
    - Requirement that the provider restrict access to PII to the authorized staff or to only those providers who require such access to perform their assigned duties;
    - Prohibition against the provider's secondary use of PII including sales, marketing or advertising;
    - Requirement that Excelsior Academy monitor and maintain control of the data;
    - Requirement that, if Excelsior Academy contract with a third party provider to collect and have access to Excelsior Academy's data as described in R277-487-3B(5), Excelsior Academy 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;
    - Requirement for data destruction and an associated timeframe; and
    - Penalties for non-compliance with the above provisions.

- Excelsior Academy's Third Party Contractors are legally allowed to engage in the following activities:
    - The use of 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 Excelsior Academy, to market the educational application or product;
    - Use 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;
    - Respond 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;

    - Use student data to allow or improve the operability and functionality of the third party contractor's internal application.

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

- A third party contractor may not (except as provided in Subsection 6(b) of the Utah Student Data Protection Act):
    - Sell student data;
    - 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 Excelsior Academy; or
    - Use student data for targeted advertising.

- A person may obtain student data through the purchase of, merger with, or otherwise acquiring a third party contractor if the third party contractor remains in compliance with state and federal law, this plan, and Excelsior Academy's previous contract with the original third party.

- The provisions of this section of Excelsior Academy's *Student Data Privacy and Security 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 the Utah SDPA.

Data Breach Protocols

Excelsior Academy shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, Excelsior Academy staff shall follow industry best practices in responding to the breach. Furthermore, Excelsior Academy 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 Executive Director or Student Data Privacy Manager who will collaborate with appropriate Excelsior Academy administrators to determine whether a security breach has occurred.
- If the Excelsior Academy administrative team determines that one or more employees or contracted partners have substantially failed to comply with this plan 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 security breaches that involve the Student Data Privacy Manager must be reported directly to the Executive Director.
- Concerns about security breaches that involve the Executive Director must be reported directly to the President of Excelsior Academy's Board of Trustees.

- Excelsior Academy will provide and periodically update, in keeping with industry best practices, resources for Utah LEAs in preparing for and responding to security breaches.

Record Retention and Expungement

Excelsior Academy staff 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 the Utah Division of Archive and Record Services. I

- In accordance with 53A-1-1407, Excelsior Academy shall expunge student data that is stored upon the request of a student, if the student is at least 23 years old.
- Excelsior Academy may expunge medical records and behavioral test assessments.
- Excelsior Academy will not expunge student records of grades, transcripts, or records of a student's enrollment or assessment information except as allowed by law.
- Excelsior Academy will collaborate with Utah State Archives and Records Services in updating data retention schedules. Student-level discipline data will be expunged after three years.

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 plan is structured to encourage the effective and appropriate use of educational data. Excelsior Academy 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, Excelsior Academy establishes clear guidelines for data collection and the purpose of the data request;
- Excelsior Academy'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 Student Data Privacy Manager must complete a review of the reliability, validity, and presentation of the data, and must follow all protocols in this plan related to appropriate disclosure.

Data Transparency

In accordance with the Utah SDPA, Excelsior Academy will annually publish all its disclosures of student personally identifiable information on the Utah State Meta Dictionary developed by USBE and located on the Data Gateway. Excelsior Academy will also provide a link from its webpage to the Meta Dictionary where this disclosure may be found.

General Non-Disclosure Assurances

All student data used by Excelsior Academy is protected as defined by FERPA and Utah statute. All Excelsior Academy staff must sign a *Excelsior Academy Employee and Volunteer Non-Disclosure Agreement* to verify acknowledgement, receipt, and intent to adhere to this *Data Governance Plan*.

All Excelsior Academy employees will do the following:

- Complete student data privacy and security training and abide by school policies for network use and data security and privacy;
- Understand and sign the Employee Non-Disclosure Agreement

Excelsior Academy

Non-Disclosure Agreement
(Please initial that you understand the following)

As an employee of the Excelsior Academy, I hereby affirm that:
_____I will abide by the terms of the Excelsior Academy'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 Excelsior Academy's Data Security and Privacy Fundamentals Training.

_____I will complete Excelsior Academy's Data Security and Privacy Fundamentals Training within 30 days.

Using Excelsior Academy Data and Reporting Systems
_____I will use a password-protected computer when accessing data and reporting systems, viewing student/staff records, and downloading reports

_____I will ensure that my computer is not left unattended and unlocked, especially when logged into sensitive systems or data including student or employee information

_____I will <u>not</u> share individual passwords for personal computers or data systems with anyone

_____I will log out of and close the browser after each use of Excelsior Academy data and reporting systems. Compass and gmail (Google Docs)

_____I will limit use of individual data to the purposes which have been authorized within the scope of job responsibilities

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

_____I will receive approval from the student data privacy manager for any educational websites/apps prior to creating student accounts with PII

Handling Sensitive Data

_____I will keep sensitive data on password-protected school-authorized computers

_____I will delete files containing sensitive data after working with them from my desktop, or move them to a secured Excelsior Academy server

_____I will use secure methods when sharing or transmitting sensitive data as approved by Excelsior Academy

_____I will keep any printed files containing personally identifiable information in a locked location while unattended, and use the secure document destruction service provided at Excelsior Academy when disposing of such records

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

Reporting & Data Sharing

_____I will not redisclose or share any confidential data analysis except to other authorized personnel without Excelsior Academy's expressed written consent

_____I will not publically publish any data without the approval of the Executive Director

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

_____I will not 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 expressly authorized in writing by the data owner and then only transmit data via approved methods

_____I understand that when sharing child/staff-identifying data with authorized individuals, the only approved methods are phone calls or Excelsior Academy's Secure File Transfer Protocol (SFTP)

_____I will immediately report any data breaches, suspected data breaches, or any other suspicious activity related to data access to my supervisor and the Excelsior Academy Student Data Manager. Moreover, I acknowledge my role as a public servant and steward of student/staff information, and affirm that I will handle personal information with care to prevent disclosure

Consequences for Non-Compliance

_____I understand that access to the Excelsior Academy 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 Excelsior Academy, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of Excelsior Academy without the prior written permission of the Student Data Manager of Excelsior Academy

Print Name: _____

Signed: _____Date: _____

References:

Policy Review Schedule (Reviewer):

Policy Monitoring Schedule (Monitor):

Document History:

Adopted: October 4, 2017

Board Chair