Table of Contents

1 PURPOSE and GOVERNING PRINCIPLES

Ogden Preparatory Academy (OPA) takes seriously its moral and legal responsibility to protect student privacy and ensure data security. 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 risks in information means there is a financial liability inherent in all data or content that is based on regulatory and ethical misuse or mismanagement.

2 SCOPE AND APPLICABILITY

This policy is applicable to all employees, temporary employees, and contractors of OPA. The policy must be used to assess agreements made to disclose data to third-parties. This policy must also be used to assess the risk of conducting business. 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.
This OPA Data Governance Plan:

Return to Table of Contents

- Designates access for all confidential information.
- Complies with all legal, regulatory, and contractual obligations regarding privacy of OPA data. Where such requirements exceed the specific stipulation of this policy, the legal, regulatory, or contractual obligation shall take precedence.
- Provides the authority to design, implement, and maintain privacy procedures meeting OPA standards concerning the privacy of data in motion, at rest and processed by related information systems.

3 DATA GROUPS

3.1 Roles

OPA's Principal, or designee, shall designate an individual as an Information Security Officer, and as a Student Data Manager.

3.2 Responsibilities

Role	Responsibilities
OPA Student Data Manager	1. Authorizes and manages the sharing, outside of the education entity, of personally identifiable student data. 2. Acts as the primary local point of contact for the USBE Student Data Officer and for state student data security administration. 3. Ensures the following notices are available to parents: a. Annual FERPA notice b. Directory Information Policy c. Survey Policy and Notice d. Data Collection Notice 4. 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,

Return to Table of Contents

	5. May **not** share personally identifiable student data for the purpose of external research or evaluation. 6. Create and maintain a list of all LEA staff that have access to personally identifiable student data. 7. Ensures annual OPA level training on data privacy to all staff members. Provide training to volunteers as appropriate. Document all staff names, roles, and training dates, times, locations, and agendas. 8. By October 1 of each year, the data manager will report to USBE the completion status of the annual confidentiality training.
IT Systems Security Manager	1. Acts as a point of contact for the USBE Student Data Officer and for state student data security administration. 2. Provides for necessary technical assistance, training, and support. 3. Oversees the adoption of the CIS Controls or comparable security controls. 4. Ensures compliance with security systems laws throughout the public education system, including: a. Providing training and support to applicable OPA employees; and b. Producing resource materials, model plans, and model forms for OPA systems security; 5. Investigates complaints of alleged violations of systems breaches; 6. Provides an annual report to the OPA Board on OPA's systems' security needs
Employees	1. Comply with all OPA, State and Federal regulations; 2. Report possible violations and breaches; 3. Attend trainings

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 OPA board members and employees must sign and comply with the OPA Employee Non-Disclosure Agreement. Contractors and volunteers, who have access to any OPA Data Systems, must sign and comply with the OPA Employee Non-Disclosure Agreement.

Return to Table of Contents

4.2 Non-Compliance

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

4.3 Non-Disclosure Assurances

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

1. Complete a Security and Privacy Fundamentals Training.
2. Use password-protected school-authorized computers when accessing any student-level or staff-level records.
3. Use Secure Networks when accessing any student-level or staff-level records. Secure Networks are home or public networks using a minimum of WPA security protocols. (WEP security protocols are not considered secure.) VPN services should be used on open networks or networks which do not meet the minimum security requirements. The IT Systems Security Officer will assist employees with necessary VPN services.
4. NOT share individual passwords for personal computers or data systems with anyone without express permission from the OPA Student Data Manager.
5. Log out of any data system/portal and close the browser after each use.
6. Lock devices when not in use or possession.
7. NOT allow anyone to use a computer or data system that is logged in under an individual account that is not the users.
8. Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.
9. Store sensitive data in appropriate-secured locations. Unsecured access and flash drives, or other removable media, or personally owned computers or devices are not deemed appropriate for storage of sensitive, confidential or student data.
10. Delete files containing sensitive data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties.

Return to Table of Contents

11. Keep printed reports with personally identifiable information in a locked location while unattended, and use the secure document destruction service provided at OPA when disposing of such records.
12. 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.
13. Redact any personally identifiable information when sharing sample reports with general audiences, in accordance with the Protecting PII in Public Reporting procedure.
14. Take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.
15. NOT use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information outside the ogdenprep.org system. 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 OPA Student Data Privacy Manager should be consulted. Email sent within the ogdenprep.org system is secure.
16. Use secure methods when sharing or transmitting sensitive data outside OPA systems. The approved method is USBE's Secure File Transfer Protocol (SFTP) website. If the SFTP is not available for the purpose of sharing data, consult with the Student Data Manager and the IT Systems Security Manager. Sharing within the OPA Network's secured server folders is appropriate for OPA internal file transfer.
17. NOT transmit child/staff-level data externally unless expressly authorized in writing by the data owner and then only transmit data after appropriate redaction and protections are in place.

4.4 DATA SECURITY AND PRIVACY TRAINING

4.4.1 Purpose

Ogden Preparatory Academy will provide a range of training opportunities for all Ogden Preparatory Academy 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 Policy

1. All OPA board members, employees, and contracted partners must sign and comply with the OPA Employee Non-Disclosure Agreement.

Return to Table of Contents

2. All current OPA board members, employees, and contracted partners are required to participate in an annual Security and Privacy Fundamentals Training.
3. The Student Data Manager and IT Systems Security Manager will identify groups in need of additional training and determine needed training.
4. Participation in the training as well as a signed copy of the OPA Employee Non-Disclosure Agreement will be annually monitored by Human Resources. Human Resources will annually report all OPA board members, employees, and contracted partners who do not have these requirements completed to the IT Systems Security Manager.

5 DATA SHARING

Providing data to persons and entities outside of the OPA 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 OPA. 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.

5.1 Procedure

1. The Student Data Manager shall approve all data sharing or designate other individuals who have been trained on compliance requirements with FERPA.
2. OPA Teachers may share individual student data with a student's parent(s) or legal guardian(s) unless legal documentation restricts the sharing of such information.
3. The Student Data Manager and the IT Systems Security Manager shall maintain the OPA metadata dictionary using the Utah Student Privacy Alliance.
    a. OPA employees shall send requests for website usage to the IT Systems Security Manager.
4. The Special Education Director may disclose Special Education data in accordance with federal and state laws and regulations.
5. 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).
6. After sharing from individual student records, the data manager shall make a note in the student record of the exchange in accordance with 34 CFR 99.32.

Return to Table of Contents

5.1.1 Electronic Communication

Ogden Preparatory Academy uses contact information to send communication to the parents/guardians of OPA students. OPA may provide contact information to certain third party vendors in order to provide parents/guardians with general information about upcoming events/services. OPA will not sell or provide parent/guardian contact information to any third party vendor as a means of promoting or selling a service. Parents/guardians may opt-out of Ogden Preparatory Academy's electronic communication service at any time. Parents/guardians may opt-out of any third party vendor service related to OPA at any time.

5.2 Security

Data shall be provided using a secure method. Secure methods include encryption and secure data sharing sites. The IT Systems Security Manager will ensure that data shared within OPA is secure.

5.3 Policy for disclosure of Personally Identifiable Information (PII)

5.3.1 Student or Student's Parent/Guardian Access

In accordance with FERPA regulations 20 U.S.C. § 1232g (a)(1) (A) (B) (C) and (D), OPA will provide parents with access to their child's education records, or eligible students access to their 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). Access shall be provided within 45 days of receiving an official request. OPA is not required to provide data that it does not maintain, nor is OPA required to create education records in response to an eligible student's request.

5.3.2 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.

Return to Table of Contents

All third-party vendors contracting with OPA 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 OPA without third-party verification that they are compliant with federal and state law, and board rule.

5.3.3 Governmental Agency Requests

OPA 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 of the federal or state requirements to share data in order to satisfy FERPA disclosure exceptions.

5.4 Dissemination Of Information About Juvenile Offenders

Upon receipt of information about juvenile offenders, the principal shall:

1. Share information about the offender and the victim with staff members who need to know for the safety of students and staff.
2. Keep this information in a secure file available only to those with a need to know. This file should be separate from the student's permanent file.

6 DATA BREACH

6.1 Policy and Procedures

OPA shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, OPA staff shall follow industry best practices for responding to the breach. Further, OPA shall follow best practices for notifying affected parties, including parents and/or legal guardians.

1. Concerns about security breaches must be reported immediately to the IT Systems Security Manager. Concerns about security breaches that involve the IT Systems Security Manager must be reported immediately to the Principal or Student Data Manager.
2. The IT Systems Security Manager will
    a. begin tracking the incident and log all information and evidence related to the investigation.
    b. collaborate with appropriate members of the OPA administrative team to determine whether a security breach has occurred.

Return to Table of Contents

c. coordinate with other IT staff to determine the root cause of the breach and close the breach.
d. coordinate with legal counsel, if necessary, to determine if the incident is meets the legal definition of a significant breach as defined in R277-487 and determine which entities and individuals need to be notified.
    i. If law enforcement is notified and begins an investigation, the IT Systems Security Manager will consult with them before notifying parents or the public so as to not interfere with the law enforcement investigation.

3. If the OPA data breach response team (Administration and the IT Systems Security Manager) determines that one or more employees or contracted partners have substantially failed to comply with OPAs IT Security Policy and relevant privacy policies, they will identify appropriate consequences, which may include termination, of employment or contract, and/or further legal action.

7 RECORD MANAGEMENT, 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 Policy

Ogden Preparatory Academy personnel shall ensure that proper student records are created, obtained, and maintained in accordance with state, federal, USBE, and OPA policy.

7.2.1 Records Management

1. Records may be maintained digitally or physically. Student education records shall contain at a minimum the birth certificate, immunization records, transcripts, and attendance records. When a student withdraws from OPA the following shall occur:
    - Applicable student records, including the request for records from the receiving school/LEA, shall be archived according to the OPA retention schedules.
        - If a request for records is not received, OPA personnel shall record information regarding student plans of transfer. Information shall include name and contact information of informant and expected destination.
    - Copies of records shall be sent to the requesting school/LEA.

Return to Table of Contents

- The student information system shall be updated to reflect the appropriate withdrawal/transfer code and exit date.

2. Parents/guardians have the right to inspect and review all of their student's education records maintained by the School. If the education records of a student contain information on more than one student, the parent/guardian may inspect and review or be informed of only the specific information about their student.
    - The School will grant a request by a parent/guardian for access to the education records of their child within a reasonable period of time, but in no case more than forty-five (45) days after the request has been made.
3. Parents/guardians may challenge and request the School to amend any portion of their student's education record that is inaccurate, misleading or in violation of the privacy rights of the student.
    - The School shall consider the request and decide whether to amend the records within a reasonable amount of time. If the Principal decides not to amend the record as requested, the Principal shall inform the parent/guardian of the decision and of their right to a hearing.
    - Upon request of a parent or guardian, the School shall provide an opportunity for a hearing to challenge the content of the Student's education records on the grounds that the information contained in the education records is inaccurate, misleading, or in violation of the privacy rights of the student.
    - Such hearing shall be informal and shall be conducted by an individual who does not have a direct interest in the outcome of the hearing.
    - If, as a result of the hearing, the School decides that the challenged information is inaccurate or misleading, the record should be amended accordingly and the parent/guardian informed in writing.
    - If, as a result of the hearing, the School decides that the challenged information is not inaccurate or misleading, it shall inform the parent/guardian of their right to place a statement in any record, commenting on the challenged information in the record, or stating why they disagree with the decision. Any such document must remain with the contested part of the record for as long as the record is maintained, and shall be disclosed whenever the portion of the record to which the statement relates is disclosed.
4. The School may not disclose information related to education records without prior parental consent, except as provided by law. Such exceptions include, but are not limited to disclosures:
    - To school officials who have a legitimate educational interest;
    - To a person or company with whom the School has contracted to perform a special task;
    - To other schools that have requested the records and in which the student seeks or intends to enroll, or where the student is already enrolled, so long as the disclosure is for purposes related to the student's enrollment or transfer;
    - To individuals who have obtained court orders or subpoenas;
    - To individuals who need to know in cases of health and safety emergencies;

Return to Table of Contents

- To officials in the juvenile justice system;
- In connection with audit and evaluation of federally or state supported education programs;
- To the Immigration and Naturalization Service (INS) for foreign students attending school under a visa; or
- To the Attorney General of the United States in response to an ex parte order in connection with the investigation or prosecution of terrorism crimes.

5. The School may disclose directory information for appropriate reasons if it has given parents annual notice of their right to request that their student's directory information not be released by the School.
    - The following information relating to students may be declared directory information from time to time:
        - Name, address, e-mail address, and telephone number;
        - Date and place of birth;
        - Major field of study;
        - Participation in officially recognized activities and sports;
        - Weight and height of members of athletic teams;
        - Dates of attendance;
        - Degrees and awards received;
        - Most recent previous educational agency or institution attended; and
        - Photograph
    - The School shall not release directory information to any individual or organization for commercial use.
6. The School shall give full rights to student education records to either parent or guardian, unless the School has been provided with evidence that there is a court order or other legally binding instrument relating to matters such as divorce, separation, or custody that specifically revokes these rights.

7.2.2 Confidentiality of Student Information

The School and all employees, volunteers, third party contractors, or other agents of the School shall protect the privacy of the student and the student's family through compliance with the protections established under state and federal law.

The School will provide appropriate training to employees regarding the confidentiality of student performance data and personally identifiable student information.

Return to Table of Contents

7.2.3 Record Disposal

Ogden Preparatory Academy shall retain and dispose of student records in accordance with OPA's Data Retention Schedule.

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

7.2.4 Expungement Requests

The procedure for expungement shall match the record amendment procedure found in 34 CFR 99, Subpart C of FERPA.

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

Return to Table of Contents

3. Expungement:
    a. If the decision is to expunge the record, OPA will seal the record or information, or make it otherwise unavailable to other staff and educators.

8 QUALITY ASSURANCES AND TRANSPARENCY REQUIREMENTS

The OPA Data Governance Plan is structured to encourage the effective and appropriate use of educational data. 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 Data Auditing

OPA personnel will work with USBE Data and Statistics Analysts in performing regular and ad hoc data auditing. OPA employees shall conduct an audit of the effectiveness of the controls used to follow the Data Governance Plan.

9 PUBLICATION POLICY

1. This policy shall be posted on the OPA website.
2. The OPA metadata dictionary shall be available via the OPA website.

Document History

Approved:	12/14/2017	
Revised:	12/12/2019	*Brought into compliance with the USBE Data Governance Plan guidance. Removed redundancies, added juvenile defender information dissemination and the requirement of CIS Controls.*
Revised:	08/18/2022	*Revised to include Records Management, previously its own policy.*

Legal References

Utah's Student Data Protection Act (SDPA)
U.C.A §53A-1-1401
63G-2-604
53A-1-1407
Family Educational Rights and Privacy Act (FERPA)
34 CFR Part 99

Return to Table of Contents

20 U.S.C. § 1232g
R277-419-9

Return to Table of Contents