Table of Contents

1 PURPOSE

Ogden Preparatory Academy (OPA) takes seriously its moral and legal responsibility to protect student privacy and ensure data security. Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401 requires that Ogden Preparatory Academy adopt a Data Governance Plan.

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:

- Designates the IT Director and the Student Data Manager as the Data Steward for all confidential information maintained within OPA.
- Designates access for all confidential information.
- Requires the Data Steward to maintain a record of all confidential information.
- Requires the Data Steward to manage confidential information according to this policy and all other applicable policies, standards and plans.

Return to Table of Contents

- 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.
- Ensures that all OPA board members and employees undergo annual privacy training.

3 DATA GROUPS

3.1 Roles

Roles are by appointment by OPA's Principal, or designee.

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. May share personally identifiable student data that are: a. of a student with the student and the student's parent b. required by state or federal law c. in an aggregate form with appropriate data redaction techniques applied d. for a school official e. for an authorized caseworker or other representative of the Department of Human Services or the Juvenile Court f. in response to a subpoena issued by a court. g. directory information h. submitted data requests from external researchers or evaluators, 4. May **not** share personally identifiable student data for the purpose of external research or evaluation. 5. Create and maintain a list of all LEA staff that have access to personally identifiable student data.

Return to Table of Contents

	6. Ensure 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.
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. 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; 3. Investigates complaints of alleged violations of systems breaches; 4. 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.

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

Return to Table of Contents

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, DVD, CD-ROM or other removable media, or personally owned computers or devices are not deemed appropriate for storage of sensitive, confidential or student data.
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.
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

Return to Table of Contents

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 Ogden Preparatory Academy board members, employees, and contracted partners must sign and follow the Staff Acceptable Use of School Electronic Resources Acknowledgement of Receipt and Understanding.
2. All OPA board members, employees, and contracted partners must sign and comply with the OPA Employee Non-Disclosure Agreement.
3. Employees that do not comply may not be able to use OPA networks or technology; non-compliance may result in termination.
4. All current OPA board members, employees, and contracted partners are required to participate in an annual Security and Privacy Fundamentals Training.
5. The Student Data Manager and IT Systems Security Manager will identify groups in need of additional training and determine needed training.
6. 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

Return to Table of Contents

partners who do not have these requirements completed to the IT Systems Security Manager.

5 Data Disclosure

5.1 Purpose

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.

5.2 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,

Return to Table of Contents

administrators, health staff, counselors, attorneys, clerical staff, trustees, members of committees and disciplinary boards, and a contractor, consultant, volunteer or other party to whom the school has outsourced institutional services or functions.
All third-party vendors contracting with 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 Policy for External disclosure of Non-Personally Identifiable Information (PII)

5.4.1 Scope

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

5.4.2 Student Data Disclosure Risk Levels

Ogden Preparatory Academy has determined three levels of data requests with corresponding policies and procedures for appropriately protecting data based on risk: Low, Medium, and High. The Student Data Manager and/or the IT Systems Security Manager will make final determinations on classification of student data requests' risk level.

5.4.2.1 Low-Risk Data

Definition: High-level aggregate data
Examples:

- DIBELS Typical Growth percentages for second-graders.
- Percent of third-graders scoring proficient on the SAGE ELA assessment

5.4.2.2 Medium-Risk Data

Return to Table of Contents

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

Examples:

- Percent of fourth-graders scoring proficient on the SAGE Mathematics assessment by ethnicity.
- Child Nutrition Program Free or Reduced Lunch percentages by class.

5.4.2.3 High-Risk Data

Definition: Personally identifiable student-level data.

Examples:

- Student-level graduation data
- Student-level SAGE ELA assessment scores for grades 3-6.

5.5 Data Request Process:

- Requester creates a Data Request ticket.
- Data Request risk level is determined by Student Data Manager and IT Systems Security Manager.
- Data Request is reviewed according to risk level:
    - Low-Risk Level: Reviewed and approved by Student Data Manager or IT Systems Security Manager
    - Medium-Risk Level: Reviewed and approved by Student Data Manager and IT Systems Security Manager
    - High-Risk Data: Request is reviewed by the School Administrative Team, if approved, request is sent to the Board for approval.
- Approved Data Requests processed by Student Data Manager.
        - Collects requested data.
        - Uses the OPA Quality Control Checklist and applies appropriate disclosure avoidance techniques. Works with IT Systems Security Manager to verify security as necessary.
        - Saves the dataset in a secure folder managed by the Student Data Manager.
        - Closes the ticket.
- Unapproved Data Requests
        - The IT Systems Security Manager and the Student Data Manager make notifications to requester and work with requestor as necessary to make adjustments for approval.

Return to Table of Contents

5.6 Data Disclosure to a Requesting External Researcher or Evaluator

Research proposals are sent directly to the Student Data Manager for review.

The Student Data Manager will ensure the proper data are shared with external researcher(s) or evaluator(s) to comply with federal, state, and board rules.

Ogden Preparatory 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 audit or evaluation. Data that do not disclose PII may be shared with external researchers or evaluators for projects unrelated to federal or state requirements if:

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

6 Data Breach

6.1 Purpose

Prompt response is essential for minimizing the risk of any further data loss and plays an important role in mitigating any negative consequences of the breach, including potential harm to affected individuals.

6.2 Policy

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.

Concerns about security breaches must be reported immediately to the IT Systems Security Manager who will collaborate with appropriate members of the OPA administrative team to

Return to Table of Contents

determine whether a security breach has occurred. 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. Concerns about security breaches that involve the IT Systems Security Manager must be reported immediately to the Principal or Student Data Manager.

7 Record Retention and Expungement

7.1 Purpose

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

7.2 Policy

- 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.
- OPA maintained student-level discipline data will be expunged three years after the student has left OPA.

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.

Return to Table of Contents

8.1 Data Collection

Where possible, data is collected at the lowest level available (i.e. at the student/teacher level). Thus, there are no aggregate data collections if the aggregate data can be derived or calculated from the detailed data.

8.2 Data Auditing

OPA personnel will work with USBE Data and Statistics Analysts in performing regular and ad hoc data auditing. Auditing analyzes the data for anomalies, investigates the source of the anomalies, and works to explain and/or correct the anomalies. OPA personnel and USBE Data Analysts also work to address findings from the Auditors.

9 Data Transparency

The IT Systems Security Manager works with the Student Data Manager to maintain the Metadata Dictionary as described in Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401

Document History

Approved: 12/14/2017

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
20 U.S.C. § 1232g

Return to Table of Contents