Policy Procedure Manual

Document Name: Data Governance Plan
First Approved Date: October 1, 2017
Latest Approved Date: January 22, 2020
Version Number: 2

1.0 Purpose

Data governance is an organizational approach to data and information management that is formalized as a set of policies and procedures that encompass the full life cycle of data, from acquisition, to use, to disposal. Wasatch Waldorf Charter School takes seriously its moral and legal responsibility to protect student privacy and ensure data security. Utah's Student Data Protection Act (SDPA), Utah Code §53A-1-1401, et seq., requires that Wasatch Waldorf Charter School adopt a Data Governance Plan.

2.0 Definitions

" Wasatch Waldorf" or "WCS" refers to Wasatch Waldorf Charter School and its governing board.

"CIS Controls" refers to the cyber security framework developed by the Center for Internet Security found at http://www.cisecurity.org/controls/.

"Metadata dictionary" means a record that: (a) defines and discloses all personally identifiable student data collected and shared by WCS; (b) comprehensively lists all recipients with whom WCS has shared personally identifiable student data, including: (i) the purpose for sharing the data with the recipient (ii) the justification for sharing the data, including whether sharing the data was required by federal law, state law, or local directive; and (iii) how sharing the data is permitted under federal or state law; and (c) without disclosing personally identifiable student data, is displayed on WCS's website.

"Personally identifiable information" or "PII" means student data that identifies or is used by the holder to identify a student. PII includes: a student's first and last name; the first and last name of a student's family member; a student's or a student's family's home or physical address; a student's email address or other online contact information; a student's telephone number; a student's social security number; a

student's fingerprint; a student's health or disability data; a student's education entity student identification number; a student's social media username and password or alias; a combination of a student's last name or photograph with other information that together permits a person to contact the student online; information about a student or a student's family that a person collects online and combines with other personally identifiable student data to identify the student; and other information that is linked to a specific student that would allow a reasonable person in the school community, who does not have first-hand knowledge of the student, to identify the student with reasonable certainty.

3.0 Policy Content

3.1 Governing Principles

WCS) takes its responsibility toward student data seriously. 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 that are ultimately responsible for data and content assets.
· **Liability:** There is risk of financial liability inherent in all data or content based on regulatory and ethical misuse or mismanagement.

3.2. Data Maintenance and Protection Policy

WCSrecognizes that there is risk and potential liability in maintaining student data and other education-related data and will incorporate reasonable data industry best practices to mitigate this risk.

3.2.1 Process

In accordance with R277-487, WCS:

· Designates _____l as its Information Security Officer.
· Adopts the CIS Controls

· Reports to the USBE by October 1 each year regarding the status of the adoption of the Center for Internet Security controls or comparable controls, and future plans for improvement.

3.3 Roles and Responsibilities Policy

WCS acknowledges the need to identify parties who are ultimately responsible and accountable for data and content assets. These individuals and their responsibilities are as follows:

3.3.1 Data Manager roles and responsibilities

· authorize and manage the sharing, outside of WCS, of PII for WCS students as described in this section
· provide for necessary technical assistance, training, and support
· act as the primary local point of contact for the state student data officer
· ensure that the following notices are available to parents:
  - annual FERPA notice (see 34 CFR 99.7),
  - directory information policy (see 34 CFR 99.37),
  - survey policy and notice (see 20 USC 1232h and Utah Code 53E-9-203),
  - data collection notice (see Utah Code 53E-9-305)

3.3.2 Information Security Officer

· Oversee adoption of the CIS Controls
· Provide for necessary technical assistance, training, and support as it relates to IT security

3.4 Training and Support Policy

WCS recognizes that training and supporting educators and staff regarding federal and state data privacy laws is a necessary control to ensure legal compliance.

3.4.1 Procedure

1. The Data Manager will ensure that employees who have access to student records or student data will receive an annual training on confidentiality of student data. The content of this training will be based on the Data Sharing Policy set forth below in section 3.6. 2. By October 1 each year, the Data Manager will report to USBE the completion status of the annual confidentiality training and provide a copy of the training materials used. 3. 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.

3.5 Audit Policy

In accordance with the risk management priorities of WCS, WCS or its designee will conduct an audit of:

· The effectiveness of the controls used to follow this data governance plan; and · Third-party contractors, in accordance with WCS's contracts with those third-party contractors. WCS's contracts with third-party contractors shall comply with the requirements of 53E-9-309(2), including the right to audit the contractors' compliance with student data privacy requirements.

3.6 Data Sharing Policy

There is a risk of redisclosure whenever student data are shared. WCS shall follow appropriate controls to mitigate the risk of redisclosure and to ensure compliance with federal and state law.

3.6.1 Procedure

3.6.1.1. The Data Manager shall approve all data sharing or designate other individuals who have been trained on compliance requirements with FERPA.

3.6.1.2. For external research, the Data Manager shall ensure that the research study follows the requirements of FERPA's study exception described in 34 CFR 99.31(a)(6).

3.6.1.3. After sharing student records or data, the Data Manager shall ensure that an entry is made in the Metadata Dictionary to record that the exchange happened.

3.6.1.4. After sharing student records (other than a typical sharing for assessment or tracking or student work purposes), the Data Manager shall make a note in the student record of the exchange in accordance with 34 CFR 99.32.

3.7 Expungement Request Policy

WCS recognizes the risk associated with data following a student year after year that could be used to mistreat the student. WCS shall review all requests for records expungement from parents and make a determination based on the following procedure.

3.7.1 Procedure

The following records may not be expunged: grades, transcripts, a record of the student's enrollment, assessment information.

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

1. If a parent believes that a record is misleading, inaccurate, or in violation of the student's privacy, they may request that the record be expunged.
2. WCS shall decide whether to expunge the data within a reasonable time after the request. 3. If WCS decides not to expunge the record, it will inform the parent of its decision as well as the right to an appeal hearing.
4. WCS shall hold the appeal hearing within a reasonable time after receiving the request for a hearing.
5. WCS shall provide the parent notice of the date, time, and place in advance of the hearing. 6. WCS shall appoint a hearing officer to conduct the hearing. The hearing officer shall be any individual who does not have a direct interest in the outcome of the hearing and may include a WCS official.
7. The hearing officer 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.
8. WCS shall make its decision in writing based exclusively on the evidence presented at the hearing, within a reasonable time following the hearing. WCS will provide a written summary of the evidence presented at the hearing, and the reasons for its decision.
9. If the decision is to expunge the record, WCS will seal it or make it otherwise unavailable to other staff and educators.

3.8. Data Breach Response Policy

WCS shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, WCS staff shall follow industry best practices for responding to the breach.

3.8.1 Procedures

3.8.1.1. The School's Executive Directorwill work with the Information Security Officer to designate individuals to be members of a cyber incident response team (CIRT).
3.8.1.2. At the beginning of an investigation, the Information Security Officer will begin tracking the incident and log all information and evidence related to the investigation.
3.8.1.3. The Information Security Officer will call the CIRT into action once there is reasonable evidence that an incident or breach has occurred.
3.8.1.4. The Information Security Officer will coordinate with other IT staff to determine the root cause of the breach and close the breach.
3.8.1.5. The CIRT will coordinate with legal counsel to determine if the incident meets the legal definition of a significant breach as defined in R277-487 to mean a breach that was intentional, that compromises a large number of student records, or that compromises sensitive records. The CIRT shall determine which entities and individuals need to be notified.
3.8.1.6. If law enforcement is notified and begins an investigation, the CIRT will consult with them before notifying parents or the public so as to not interfere with the law enforcement investigation.

3.9 Publication Policy

WCSrecognizes the importance of transparency and will post this policy on its website.

4.0 Exhibits / Appendices / Forms

FERPA

FERPA is a federal law that protects the privacy interests of students. It affords parents the right to access and request that their children's education records be amended, and gives them some control over the disclosure of the information in these records. FERPA generally prevents schools from sharing student records, or personally identifiable information in these records, without the written consent of a parent, except as provided by law.

At WCS we respect student and family privacy, which means that we never discuss an individual student with a member of the staff, another teacher, or a parent if that individual is not someone who has a legitimate need to know. This is particularly true of any situation involving grades, evaluations, or assessments; student discipline; student health; or aspects of a student's home or family situation.

Notwithstanding anything in this policy, when a school employee believes that a situation exists which presents a serious threat to the well-being of the student, the employee must notify the student's parent or guardian without delay, unless the matter has already been reported to DCFS, in which case it is the responsibility of DCFS to notify the student's parent or guardian of any possible investigation or take other appropriate action.

Notwithstanding anything in this policy, when a school employee believes that a student is at-risk of attempting suicide, physical self-harm, or harming others, the employee may intervene and ask the student questions regarding the student's suicidal thoughts, physical self-harming

behavior, or thoughts of harming others for the purposes of (1) referring the student to appropriate prevention services, and (2) informing the parent or legal guardian.

I understand that by the virtue of my agreement to work at Wasatch Waldorf Charter School, I may have access to records which contain individually identifiable information such as a social

security number or student identification number, of which the disclosure is prohibited by the Family Educational Rights and Privacy Act of 1974 (FERPA). FERPA is a Federal regulation that governs the privacy and disclosure of student records. I acknowledge that I fully understand that no student information is to be released to non-district personnel or third-parties. The intentional disclosure by me of this information violates FERPA policy and could subject me to criminal and civil penalties imposed by law. I further acknowledge that such willful or unauthorized disclosure could constitute just cause for termination of my volunteer services immediately regardless of whether criminal or civil penalties are imposed.

In relation to my work, I must follow the guidelines outlined above. If my assigned responsibilities include access to student files, data, or information, I will abide by the confidentiality and privacy policies of WCS. I understand that if I have any questions regarding the disclosure of information, I must ask WCS administration prior to sharing any observations or information obtained in the course of my service.

Non Disclosure Assurances

I understand that as an employee of Wasatch Waldorf Charter School (including contract or temporary employees) I will:

1. Complete a Security and Privacy Fundamentals Training.
2. Complete a Security and Privacy Training for Researchers and Evaluators, if your position involves research analysis or if requested by Wasatch Waldorf Charter

School Management or Administration.

3. Consult with Wasatch Waldorf Charter School internal data owners when creating or disseminating reports containing data.

4. Use password-protected state-authorized computers when accessing any student-level or staff-level records.

5. NOT share individual passwords for personal computers or data systems with anyone.

6. Log out of any data system/portal and close the browser after each use.

7. Store sensitive data on appropriate-secured location. Unsecured access and flash drives, DVD, CD-ROM or other removable media, or personally owned computers or devices are not deemed appropriate for storage of sensitive, confidential or student data.

8. Keep printed reports with personally identifiable information in a locked location while unattended, and use the secure document destruction service provided at Wasatch Waldorf Charter School when disposing of such records.

9. NOT share personally identifying data during public presentations, webinars, etc. If users need to demonstrate child/staff level data, demo records should be used for such presentations.

10. Redact any personally identifiable information when sharing sample reports with general audiences, in accordance with guidance provided by the student data manager.

11. Take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.

12. Delete files containing sensitive data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties.

13. NOT use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If users receive an email containing such

information, they will delete the screenshots/text when forwarding or replying to these messages. If there is any doubt about the sensitivity of the data the Student Data Privacy Manager should be consulted.

14. Use secure methods when sharing or transmitting sensitive data. The approved method is sending with password protection. Also, sharing within secured server folders (such as on Google Drive) is appropriate for Wasatch Waldorf Charter School internal file transfer.

15. NOT transmit child/staff-level data externally unless expressly authorized in writing by the data owner and then only transmit data via approved methods such as described in item ten.

16. Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.

Electronic Devices

Employees, parents and volunteers at Wasatch Waldorf Charter School are not to use personal electronic devices during the school day when in contact with children, unless there is an emergency situation. Devices should be placed in a silent mode and stored out of site during times when supervising and interacting with students. Cell phones and other electronic devices may be used on breaks, in meetings (as appropriate), and in emergency situations.

Electronic devices may not be used in a way that threatens, humiliates, harasses, intimidates, or violates local, state or federal law of school-related individuals, including students, employees,

and visitors. Electronic devices may not be used during Utah Performance Assessment System for Student assessments unless specifically allowed by law, student Individual Education Plan, or assessment directions.

Full-time teachers and other staff may be issued individual computers which are labeled and inventoried by Wasatch Waldorf Charter School. All computers, iPads, and other school property that are used by

teachers at the school or taken home to be used, are subject to standards of professional conduct. School property and networks may not be used for unprofessional activities or illegal activities, such as personal use of social media, creation or viewing of pornography, or personal business activities. While incidental personal use of school computers may occur, employees are not to store personal files, photos or information on any electronic device issued or owned by WCS.

Providing IT resources to an employee does not imply an expectation of privacy. WCS Administration or the State of Utah may:

(a) View, authorize access to, and disclose the contents of electronic files or communications, as required for legal, audit, or legitimate state operational or management purposes;

(b) Monitor the network or email system including the content of electronic messages, including stored files, documents, or communications as are displayed in real-time by employees, when required for state business and within the officially authorized scope of the person's employment.

An employee may engage in incidental and occasional personal use of IT resources provided that such use does not:

(a) Disrupt or distract the conduct of school business due to volume, timing, or frequency;

(b) Involve solicitation;

(c) Involve for-profit personal business activity;

(d) Involve actions, which are intended to harm or otherwise disadvantage the state; or

(e) Involve illegal and/or activities prohibited by this rule.

An employee shall:

(a) comply with the Government Records Access and Management Act, as found in Section 63G-2-101 et seq., Utah Code, when transmitting information with WCS provided IT resources.

(b) Report to agency management any computer security breaches, or the receipt of unauthorized or unintended information.

(4) While using WCS provided IT resources, an employee may not:

(a) Access private, protected or controlled records regardless of the electronic form without data owner authorization;

(b) Divulge or make known his/her own password(s) to another person;

(c) Distribute offensive, disparaging or harassing statements including those that might incite violence or that are based on race, national origin, sex, sexual orientation, age, disability or political or religious beliefs;

(d) Distribute information that describes or promotes the illegal use of weapons or devices including those associated with terrorist activities;

(e) View, transmit, retrieve, save, print or solicit sexually-oriented messages or images;

(f) Use state-provided IT resources to violate any local, state, or federal law;

(g) Use state-provided IT resources for commercial purposes, product advertisements or "for-profit" personal activity;

(h) Use state-provided IT resources for religious or political functions, including lobbying as defined according to Section 36-11-102, Utah Code, and rule R623-1;

(i) Represent oneself as someone else including either a fictional or real person;

(j) Knowingly or recklessly spread computer viruses, including acting in a way that effectively opens file types known to spread computer viruses particularly from unknown sources or from sources from which the file would not be reasonably expected to be connected with;

(k) Create and distribute or redistribute "junk" electronic communications, such as chain letters, advertisements, or unauthorized solicitations;

(l) Knowingly compromise the confidentiality, integrity or availability of the School's information resources.

(5) Once WCS Administration determines that an employee has violated this rule, they may impose disciplinary actions.

Training

I certify that I have participated in training provided by Wasatch Waldorf Charter School regarding Student Data Privacy. This has included: (Initial all that Apply)

_____ New Employee / Back to School Review of Handbook and Policy and Procedures

_____ Training by USBE Staff on IDEA and FERPA

_____ Security and Privacy Fundamentals Training Curriculum Module

I understand that if I have any questions regarding the information presented in any training that I must contact my supervisor or the Executive Director for clarification.

Agreements

As an employee of Wasatch Waldorf Charter School, I hereby affirm that: (Initial)

_____ I have read the Employee Non-Disclosure Assurances attached to this agreement form and read and reviewed Data Governance Plan, and all applicable Wasatch Waldorf Charter

School policies and procedures. These assurances address general procedures, data use/sharing, and data security.

_____ I will abide by the terms of the Wasatch Waldorf Charter School's board policies and corresponding plans, processes, 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. Using Wasatch Waldorf Charter School Data and Reporting Systems.

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

_____ I will not share or exchange individual passwords, for either personal computer(s) or Wasatch Waldorf Charter School system user accounts, with WCS staff or participating program staff.

_____I will log out of and close the browser after each use of Wasatch Waldorf Charter School data and reporting systems.

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

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

Handling Sensitive Data

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

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

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

_____ I will delete files containing sensitive data after working with them from my desktop, or move them to Google Drive.

Reporting & Data Sharing

_____ I will not disclose or share any confidential data analysis except to other authorized personnel without the expressed written consent of the Data Advisory Team (Executive Director, Data Manager or the Director of Student Support Services).

_____ I will not publicly publish any data without the approval of the Executive Director.

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

_____ I will not use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If I need to send PII or information from Student

Records, I will do so using password protection. If I receive an email containing such information, I will delete the sensitive information when forwarding or replying to these messages. (This means I will delete the ENTIRE previous thread from my email reply.)

_____I will not transmit student data externally (outside of WCS) unless explicitly authorized in writing by the Wasatch Waldorf Charter School Executive Director.

_____ I understand that when sharing student data with authorized individuals, the only approved methods are phone calls, password protected documents, or other secure methods as

approved by Wasatch Waldorf Charter School. Also, sharing within secured server folders is appropriate for Wasatch Waldorf Charter School internal file transfer.

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

Consequences for Non-Compliance

_____ I understand that access to the Wasatch Waldorf Charter School 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 Wasatch Waldorf Charter School, I will not disclose or otherwise disseminate any confidential or personally identifiable

information to anyone outside of Wasatch Waldorf Charter School without the prior written permission of the Executive Director of Wasatch Waldorf Charter School.

I agree to and certify that all of the preceding information is correct and that I will abide by all agreements and assurances contained therein.

Print Name: _____

Signed: _____

Date: _____

Appendix B: Protecting Personally Identifiable Information (PII) in Public Reporting

Data Gateway Statistical Reporting Method for Protecting PII

Public education reports offer the challenge of meeting transparency requirements while also meeting

legal requirements to protect each student's personally identifiable information (PII). Recognizing this, the reporting requirements state that subgroup disaggregation of the data may not be published if the results would yield personally identifiable information about an individual student. While the data used by the Utah State Board of Education (USBE) and local education agencies (LEAs) is comprehensive, the data made available to the public is masked to avoid unintended disclosure of personally identifiable information at summary school, LEA, or state-level reports.

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

1. Underlying counts for groups or subgroups totals are not reported.

2. If a reporting group has 1 or more subgroup(s) with 10 or fewer students. a. The results of the subgroup(s) with 10 or fewer students are recoded as "N<10" b. For remaining subgroups within the reporting group
    i. For subgroups with 300 or more students, apply the following suppression rules. 1. Values of 99% to 100% are recoded to ≥99%
        2. Values of 0% to 1% are recoded to ≤1%
    ii. For subgroups with 100 or more than but less than 300 students, apply the following suppression rules.
        1. Values of 98% to 100% are recoded to ≥98%
        2. Values of 0% to 2% are recoded to ≤2%
    iii. For subgroups with 40 or more but less than 100 students, apply the following suppression rules.
        1. Values of 95% to 100% are recoded to ≥95%
        2. Values of 0% to 5% are recoded to ≤5%
    iv. For subgroups with 20 or more but less than 40 students, apply the following suppression rules.
        1. Values of 90% to 100% are recoded to ≥90%
        2. Values of 0% to 10% are recoded to ≤10%
        3. Recode the percentage in all remaining categories in all groups into intervals as follows (11-19,20-29,…,80-89)

v. For subgroups with 10 or more but less than 20 students, apply the following suppression rules.

1. Values of 80% to 100% are recoded to ≥80%
2. Values of 0% to 20% are recoded to ≤20%
3. Recode the percentage in all remaining categories in all groups into intervals as follows (20-29,30-39,…,70-79)