Document Name:	Data Governance Plan
First Approved Date:	October 1, 2017
Latest Approved Date:	October 30, 2024
Version Number:	4

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 §53E-9-302, 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

WCS recognizes 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 Third Party Vendor 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 Director will 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

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

4.0 Exhibits / Appendices / Forms

5.0 Appendices