11. DATA GOVERNANCE

11.102 Employee Non-Disclosure Assurances

The Board of Education of Ogden School District recognizes employee non-disclosure assurances are intended to minimize the risk of human error and misuse of information. All Ogden School District board members, employees, contractors and volunteers must sign and adhere to the **Ogden School District Employee Non-Disclosure Agreement**.

Non-compliance with the agreements shall result in consequences up to and including removal of access to Ogden School District network; if this access is required for employment, employees and contractors may be subject to corrective action up to and including termination of employment or contracted services.

All student data utilized by Ogden School District is protected as defined by the Family Educational Rights and Privacy Act (FERPA), IDEA, Utah statute, and district policies and procedures. This policy outlines the way Ogden School District staff is to utilize data and protect personally identifiable and confidential information.

Legal Ref.: Utah's Student Data Protection Act (SDPA)
U.C.A. § 53E-9-301
FERPA and IDEA

Approved by the Board of Education: November 16, 2017.

PROCEDURE:

A signed agreement form is required from all Ogden School District staff to verify agreement to adhere to/abide by these practices and will be maintained in Ogden School District Human Resources. All Ogden School District employees (including contract, temporary, and volunteers) will:

1. Complete the job appropriate security and privacy training.
    a. Level 1 Security and Privacy Training
        i. This training is an overview of data governance and security (e.g., best practices, guidelines, policy review, etc.).
        ii. Required of all employees (including board members, contract, temporary, and volunteers).
    b. Level 2 Security and Privacy Training
        i. This training includes a fundamental understanding of data governance and security specific to users who have school-level access to student data.
        ii. Required if
            1. The position requires an educator license.
            2. The employee has school-level access to student data.
            3. Requested by the Student Data Manager.
    c. Level 3 Security and Privacy Training

11.102 Employee Non-Disclosure Assurances (cont.)

   i. This training includes an advanced understanding of data governance and security for users with district-level access to student data.
   ii. Required if
      1. The position requires an administrative license.
      2. The employee has district-wide access to student data.
      3. Requested by the Student Data Manager.

2. Consult with Ogden School District internal data owners when creating or disseminating reports containing data.
3. Take appropriate action to secure data when accessing district data on any device.
4. NOT share individual passwords for personal computers or data systems with anyone.
5. Log out of any data system/portal and close the browser after each use on any device.
6. Store sensitive data on appropriate-secured location. Unsecured or unencrypted access of 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.
7. Keep printed reports with personally identifiable information in a locked location while unattended, and use the secure document destruction service provided at Ogden School District when disposing of such records.
8. NOT share personally identifying data during public presentations, webinars, etc. If users need to demonstrate student/staff level data, demo records should be used for such presentations.
9. Redact any personally identifiable information when sharing sample reports with general audiences, in accordance with guidance provided by the student data manager.
10. Take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.
11. Delete files containing sensitive data after using them on computers
12. Move all files to secured servers, district-managed cloud storage, or personal folders accessible only by authorized parties.
13. NOT use email to externally (i.e. someone without an @ogdensd.org email address) 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. Limit the amount of personally identifiable or other sensitive information when sending email internally (i.e. someone who has an @ogdensd.org email address).
15. **NOT** email or share Personally identifiable or sensitive information to an email list (e.g. BNESStaff@ogdensd.org) even though it is an internal.
16. Use secure methods when sharing or transmitting sensitive data.
17. NOT transmit student/staff-level data externally unless expressly authorized and then only transmit data via approved methods (OSD Google Drive/Team Drive,

11.102 Employee Non-Disclosure Assurances (cont.)

Secure File Transfer Protocol (sftp) with someone who has signed data doc, or USBE MOVEit or other program deemed approved by the Chief Privacy Officer).

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

Ogden School District Employee Non-Disclosure Agreement

As an employee of the *Ogden School District*, I hereby affirm that: (Initial)

_____ I have read the Employee Non-Disclosure Assurances (Section 11.102) attached to this agreement form and read and reviewed Ogden School District Data Governance Plan policies.

_____ I acknowledge that Ogden School District may monitor the collection and retention of security related information (manually or electronically collected).

Trainings:

_____ I have completed the appropriate Ogden School District Security and Privacy Training (Level 1, 2, and/or Level 3).

Using Ogden School District Data and Reporting Systems:

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

_____ I will not share or exchange individual passwords, for either personal device(s) or Ogden School District system user account with anyone.

_____ I will lock my device whenever I leave my computer unattended.

_____ I will only access data in which I have received permission to use in order to fulfill essential job or volunteer duties.

_____ I will notify the data owner or the Ogden School District Data Manager if I become aware that I have access to data that is not needed to fulfill my essential job or volunteer duties.

_____ I will not attempt to access data, except as is required to fulfill essential job or volunteer duties.

Handling Sensitive Data:

_____ I will keep sensitive data on password-protected devices provided by Ogden School District.

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

_____ I will not share student/staff-identifying data during public presentations, webinars, etc.

_____ I will delete files containing sensitive data after working with them from my desktop or local computer drives or move them to a secure location.

11.102 Employee Non-Disclosure Assurances (cont.)

Ogden School District Employee Non-Disclosure Agreement (cont.)

Reporting & Data Sharing:

_____ I will not disclose, share, or publish any confidential data analysis without the approval of my supervisor.

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

_____ I will not use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information with someone outside of Ogden School District email domain. If I receive an email containing such information, I will delete the screenshots/text when forwarding or replying to these messages.

_____ I will limit the amount of personally identifiable or sensitive information I send to someone within the Ogden School District email Domain.

_____ I will NOT share personally identifiable or sensitive information with email lists.

_____ I understand that when sharing student/staff-identifying data with authorized individuals, the only approved methods are OSD Google Drive/Team Drive, Secure File Transfer Protocol (sftp) with someone who has signed data doc, or USBE MOVEit or other program deemed approved by the Chief Privacy Officer.

_____ I will immediately report any data breaches, suspected data breaches, or any other suspicious activity related to data access to my supervisor.

Consequences for Non-Compliance:

_____ I understand that failure to comply with the above statements may result in loss of access to network and systems and/or corrective action up to and including the termination of my employment.

_____ I agree that upon the cessation of my employment from Ogden School District, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of Ogden School District without the prior written permission of the Student Data Manager of Ogden School District.

Print Name: _____

Signed: _____

Date: _____