Elmira City School District

7244F.1

Administration Building
951 Hoffman Street
Elmira, NY 14905

Phone: (607) 735-3000
www.elmiracityschools.com

Release and/or Sharing of Student Data Form

Third-Party Contractors requesting access to student data and/or teacher or principal data ("data") must complete this form to ensure the confidentiality and security of data as required by Board of Education policy and all applicable local, state, and federal laws. Attach addendums to the questions if more space is needed

Contractor/Company Name: Northwest Evaluation Association ("NWEA")
Representative Name and Title: Amanda Towerman, Sr. Account Manager
Contractor Phone Number: 503.444.6404

1. Describe the data that is being requested and/or stored:
   Personally Identifiable Student Information includes but is not limited to student name, date of birth, Identification numbers, assigned teacher, classification data, RIT score. See NWEA Privacy and Security Policy for Student Information Addendum for additional information.

2. Exclusive purposes of the use of the data:
   Use assessment data to create, generate, and deliver reports to NWEA's subscribers.
   See NWEA Privacy and Security Policy for Student Information addendum for additional information.

3. Will any third-party subcontractors have access to the data? [X] Yes [ ] No
   If yes, how will you ensure that subcontractors, and any persons or entities that the third party subcontractor may share the data with, will abide by data protection and data security requirements?
   Third party subcontractors enter into confidentiality agreements with NWEA no less restrictive than that between NWEA and District. All such third party subcontracts must abide by all data protection/security requirements in the agreement between NWEA and District and as required by applicable law.

4. What happens to the data upon expiration of the agreement or relationship with the District?
   NWEA retains data for the length of time necessary to meet contractual and legal commitments to subscribers. Often, commitments extend past end date of agreements because subscribers require continued access to data as evidence of education data for reporting purposes as well as to maintain data for future longitudinal growth studies

5. How would a parent, student, eligible student, teacher or principal challenge the accuracy of the data that is collected or stored?
   If parent contacts NWEA to challenge accuracy of data, NWEA will contact subscriber to validate identity of the parent/guardian/student and request instructions regarding corrective action to be taken, if any. Once validated, NWEA will correct erroneous data and associated records as directed by subscriber in writing.

6. Describe where the data will be stored so as to protect data security and the security protections that will be taken to ensure such data will be protected, including whether such data will be encrypted and if so, how?
   Data is stored in a highly available and secure off-site co-locations data center located in the United States. NWEA conducts regular backups and employs industry standard environmental controls as well as encryption in transit using SSL over HTTP. Please see Web-Based MAP System Security Policy addendum for additional info.

Authorized Signature: DocuSigned by: Geri Cohen 9EE11D7374704BD... Date: August 17, 2016

FOR DISTRICT USE ONLY

Date Received: 8/19/2016
Received By: JEM

NWEA Privacy and Security Policy for Student Information

Northwest Evaluation Association ("NWEA") honors the privacy of student information and recognizes the importance of protecting such sensitive information. NWEA strives to treat personally identifiable student data ("Personal Student Data") according to applicable local laws that regulate securing the access, maintenance, and transfer of Personal Student Data. This Privacy Policy ("Policy") describes the types of student information we receive from our subscribers of our products and services and may collect from students taking NWEA assessments and our practices for collecting, using, maintaining, protecting, and disclosing that information.

Personal Student Data Collected from Subscribers

In order to perform the services pursuant to an agreement, our subscribers provide and we collect information which varies with the activity but which typically includes items such as the following:

- Full Name
- Date of Birth
- Student Identification Number Assigned by Subscriber
- Assigned Classroom Teacher
- Classification Data (which may, but does not always, include race, ethnicity, gender, nationality, free/reduced lunch)
- Disability Status for accommodation

Personal Student Data Collected from Students

As a result of students taking NWEA assessments, we collect the following information associated with each student:

- RIT scores used in system reports for subscribers
- Student Item Responses
- Growth projections

Use and Disclosure of Personal Student Data

As a vendor to subscribing schools and districts, NWEA is subject to its subscribers' privacy and security policies with regards to maintaining and transferring Personal Student Data. We are a research educational not-for-profit with a mission to partner with others to help all kids learn. We use Personal Student Data to perform services under our agreements with our subscribers and to fulfill our mission and do not repurpose Personal Student Data for sale to third parties for their commercial use. For example, we:

- Use Personal Student Data to create, generate, and deliver reports to our subscribers including custom reports as requested. In addition, we may use Personal Student Data, with subscribers'

written permission, for statistical studies and research by us or third parties to benefit our subscribers (e.g., virtual comparison group studies, linking and alignment studies)
- Subject to applicable law and under a separate permission agreement by our subscribers, we may share and transfer Personal Student Data to third parties to evaluate educational or research programs or to conduct research studies.
- Generate aggregate data, which does not identify students in particular but tends to reflect collective information about students (see below for Non-personal Student Data).
- Deal with legal processes such as subpoenas, claims of test security breach.

Non-Personal Student Data Collected

We collect and use some information from NWEA assessments in aggregate form so that it cannot be manipulated to identify any particular individual user.

- Assessment response times
- Item response times
- Assessment behavior such as completed, paused, suspended, and terminated tests

Use and Disclosure of Non-Personal Student Data

As an educational research organization and as part of providing services to its subscribers, we use Non-Personal Student Data to:

- Conduct research and produce aggregate statistical studies and analysis related to our products and services by us or third parties as an added benefit to our subscribers (e.g. Norming studies)
- To improve our products and services and our business systems and procedures, from time to time.

Retention of Data

We retain Personal Student Data for the length of time necessary to meet our contractual and legal commitments to our subscribers. Most of the time, these commitments extend past the end date of our agreements since our subscribers may need continued access to Personal Student Data as evidence of educational data for reporting and many subscribers resume their subscriptions at a later date and want their historical Personal Student Data intact for longitudinal growth studies or for legal compliance. However, we honor subscribers' requests to destroy data from our production systems upon written request.

Our customary practice is to retain Non-Personal Student Data indefinitely for the purposes stated above in "Use and Disclosure of Non-Personal Student Data" to further our mission.

Security of Data

We have established technological, internal policies and practices, and appropriate safeguards to help prevent unauthorized access to or misuse of Personal Student Data. To protect confidentiality, we employ policies and procedures around segregation of duties and personnel management to ensure Personal Student Data and other sensitive data remain secure. This includes practices around recruiting and hiring involving security clearance and background checks. All employees complete orientation and training regarding appropriate use of communications and software systems and

foundational information security policies. NWEA audits these controls regarding access, confidentiality, and integrity yearly via an SSAE 16 audit, done by an outside independent auditing firm. We also endeavor to require our service providers and other contractors to provide similar protection appropriate for the nature of the data handled by the providers.

NWEA uses industry standard methods such as SSL (secure socket layer) or encrypted file transfer techniques to secure and protect Personal Student Data and other confidential information. A multi-layered security approach protects data in storage. Internal access to confidential or sensitive data is limited to those with a need to know and who have executed a confidentiality and non- disclosure agreement. Our test delivery applications provide security and role based access at various levels of entry, analysis, and reporting. Access to the assessment system and the reports website are made available by using passwords that our subscribers define and keep secure. These passwords help us verify the subscriber's identity before granting access or making corrections to any information. As such, subscribers should never disclose their passwords to anyone. Our subscribers are responsible for maintaining the secrecy of their passwords and any information reported to them by us.

More detailed information about our Privacy and Security practices, see the document Web-Based MAP Security Specifications.

Data Breach Notifications

In the event of a security breach of Personal Student Information or other confidential information of our subscribers, we notify affected subscribers as soon as practicable in accordance with applicable laws. We have an Information Security Team that will monitor the recovery and repair of the technical or process vulnerability.

Contact Information

For additional information or concerns, please contact NWEA at Audit-Risk@nwea.org

Web-Based MAP® System Security Policy

Purpose

The purpose of this policy is to outline: (i) system security for the Web-Based MAP system; and (ii) the role users have in protecting their MAP personally identifiable information.

Scope

The responsibilities under this policy apply to all NWEA personnel and contractors who have access to NWEA information assets covered under this policy.

Portions of this policy also apply to NWEA partners and users who access and utilize the NWEA Web-Based MAP system.

System Security

The Web-based MAP® system protects users' personally identifiable MAP data by:

- Storing the MAP application system and its data in a highly available and secure off-site co-location data center located in the United States.
- Conducting regular database back-ups, which are stored in a second geographically separate secure off-site co-location facility located in the United States.
- Employing industry standard environmental controls in our data center locations, including:
    - Environmental monitoring (cooling and power);
    - UPS power;
    - Backup generator;
    - Data center fire detection and suppression; and
    - 24 hour monitored physical security.
- Encrypting MAP data in transit using Secure Sockets Layer (SSL) over Hyper Text Transfer Protocol (HTTP).
- Ensuring that MAP data is stored in privately addressed networked devices that have no direct interaction with public networks.
- Routing all incoming and outgoing traffic through a firewall, which is managed by NWEA engineers.
- Maintaining business continuity and disaster recovery plans in the event of an emergency or natural disaster that including the following:
    - Available recovery times.
    - Conducts 24x7 system monitoring that is capable of detecting potential outages.

    - Plans for File-level, Database and server recovery after a component/system failure, damage, or compromise.
    - Geographical separation between data centers hosting production, backup and redundant system elements.
    - Includes recovery/mitigation procedures for all managed sites.
    - Includes provisions for at least the following events:
        - Fire;
        - Natural disaster;
        - Sabotage;
        - Accidental human error;
        - Flooding;
        - Equipment failure; and
        - Application/database failure.
- Utilizing change management processes.
- Utilizing Microsoft Active Directory to provide administrative security boundaries for NWEA engineers, clients, and staff. All workstations are members of NWEA domains and restrict user rights to authorized business needs.
- Maintaining privacy incident and breach notification procedures.
- Conducting system level testing for new functionalities that are added to the Web-Based MAP® system to reconfirm system security measures are retained and functional.
- Conducting regular penetration testing of the system to verify security controls are working as designed.
- Employing user authentication policies that give your organization control of user names and passwords, with several special characters accepted and a password requirement of at least 8 characters.
- Deploying denial of service attack mitigation services.
- Including component and system level fault tolerance and redundancy in system design including but not limited to:
    - Redundant disk configurations on critical file systems;
    - Redundant disk controllers;
    - Dual power supplies on all critical application servers; and
    - Clustered application servers.
- System monitoring and alerting for errors, performance, CPU utilization, and storage.
- Providing an inactivity time-out feature that logs users off the Web-Based MAP® system who have been inactive or exceeded a maximum number of login attempts.
- Encrypting user passwords in any data storage location and obfuscating password entry fields in any entry interface controlled by the discloser.
- Securing transmission of login credentials.
- Enforcing role-based access based on several roles, each with specific permissions, to control implementation, configuration, data management, testing, and reporting.
- Maintaining MAP data in accordance with the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g(a)(4)(A)(ii), 1232g(b)(1) – for the primary purpose of providing assessment and research services pursuant to your agreement with NWEA.

- Notifying you of any written third party requests for disclosures of your MAP personally identifiable information. Only you may authorize actual disclosures of such personally identifiable information to third parties.
- Conducting criminal history screening of employees with access to your MAP personally identifiable information.

Protecting Personally Identifiable Information

Users are responsible for:

- Ensuring that their personnel and technology that access the Web-based MAP® system keep student data secure and comply with the Family Educational Rights and Privacy Act (FERPA).
- Password security policies, including disabling password-saving on all of your devices. Saving passwords on a shared computer can cause a security breach, making student data available to anyone who can access the computer. Saving passwords could lead to a violation state and federal regulations.
- Ensuring the security and availability of your own computers, computer networks, and Internet connections, including security patches, choice of browser, and browser configuration settings to be used with the Web-based MAP product, e-mail, and other transmissions.
- Maintaining policies to address student assessment and the use of, and access to, confidential student information.
- Configuring roles based access to MAP data in the NWEA Web-Based MAP® system in accordance with your applicable policy.
- Providing an annual notice to parents under FERPA, that (a) MAP data shall be maintained in part on behalf of you by NWEA and its contractors in order to provide assessment and research services to you; (b) NWEA employees and employees of NWEA's contractors shall be deemed school officials for the purpose of access to personally identifiable information derived from MAP data only if they have a legitimate interest in maintaining, organizing, or analyzing the data for assessment and research purposes consistent with your agreement with NWEA; and (c) personally identifiable information derived from student education records and maintained by NWEA shall not be further disclosed to third parties, except as allowed by FERPA and authorized by you or by your agreement with NWEA. You are responsible for any notices to parents required under FERPA and for providing parents/guardians with an opportunity to inspect and challenge the contents of the student records in question.
- Authorizing actual disclosures of your personally identifiable information from MAP data to third party organizations and maintaining a record of the request or disclosure with the records of each student and providing the record to parents upon request, as required by 34 CFR 99.32. If you authorizes a disclosure for a study to improve instruction, it shall authorize NWEA to enter into the required agreement with the third party organization on its behalf, consistent with 34 CFR 99.31(a)(6)(i)(C).

Ownership and Review

The NWEA Information Security Committee is responsible for any and all changes to this policy.