



AKRON PUBLIC SCHOOLS PRIVACY AND DATA SECURITY POLICY

Background

In an effort to protect the use of employee and student personally identifiable information (PII), Akron Public Schools has adopted a privacy and data security policy as outlined herein.

Statement 1

Vendor agrees that any and all data exchanged shall be used expressly and solely for the purposes of monitoring employee and student performance data to facilitate improvement. Data shall not be distributed, re-purposed, or shared across other applications, environments, or Company business units. As required by Federal and State law, Vendor further agrees that no data of any kind shall be revealed, transmitted, exchanged, or otherwise passed to other vendors or interested parties without the express written consent of the contracting Local Education Agency (LEA). Vendor will disclose Confidential Information to its employees, authorized subcontractors, agents, consultants and auditors on a “need to know” basis only, provided that all such subcontractors, agents, consultants and auditors have executed written confidentiality obligations to Vendor and all Vendor clients. The confidentiality obligations shall survive termination of any agreement with Vendor for a period of twenty (20) years or for so long as the information remains confidential, whichever is longer.

Statement 2

Vendor agrees to protect and maintain the security of data with security protection measures that include maintaining secure environments that are patched and up to date with all appropriate security updates in accordance with industry standards. In order to ensure that only appropriate individuals and entities have access to personally identifiable employee and student data, Vendor has implemented various forms of authentication including, but not limited to secure password authentication and SSL encryption to establish the identity of the requester of the information with a level of certainty that is commensurate with the sensitivity of the data. No individual or entity is allowed unauthenticated access to confidential personally identifiable employee and student records or data at any time for any reason.

Statement 3

Vendor agrees to comply with any and all State and Federal Laws, including but not limited to FERPA and COPPA, that require the notification of individuals in the event of unauthorized release of personally identifiable information or other event requiring notification. In the event of a breach of any of Vendor's security obligations or other event requiring notification under applicable law, Vendor agrees to notify impacted LEAs immediately and assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, and to hold harmless and defend the contracting LEA and its employees from and against any claims, damages, or other harm related to the breach and/or the Notification Event as applicable.

Statement 4

Vendor has established and implemented a clear data breach response plan outlining organizational policies and procedures for addressing a breach, which is an essential step in protecting the privacy of employee and student data. Prompt response is essential for minimizing the risk of any further data loss and therefore, plays an important role in mitigating any potential negative consequences of the breach, including potential harm to affected individuals. A data breach is any instance in which there is an unauthorized release or access of personally identifiable information or other information not suitable for public release.

Statement 5

Vendor agrees that upon termination of its agreement with the contracting Local Education Agency, it shall return all data in a useable electronic format, and erase, destroy, and/or render unreadable all data from the contracting LEA in its entirety in a manner that prevents its physical reconstruction through the use of commonly available file restoration utilities. Vendor further agrees to certify in writing that these actions have been completed within 60 days of the termination of the applicable agreement or within 7 days of the request of an authorized agent of LEA, whichever shall come first.

Vendor Company Name: _____

Vendor Representative: _____

Date Signed: _____ APS Employee: _____