Data Privacy and Security Statement

PARENT BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Educational Vistas, Inc. complies with and exceeds all expectations of Section 2-c and 2-d of the Education Law.

PHYSICAL SAFEGUARDS

Educational Vistas' programs and data are housed at TurnKey in Latham which is a secure data Center. TurnKey is a 24/7 monitored facility that restricts physical access to the servers. The servers are also appliance and firewall protected from outside access. There are only 3 of our technicians allowed into the data center and the data center is required to call our offices before granting anyone access to the servers. The center requires physical sign-in to the facility as well. Data is housed on multiple redundant load-balanced servers within the facility. Backed up data is encrypted and has to be restored to the data center before it can be used.

ENCRYPTION IN MOTION

The data center uses SHA-256 bit encryption along with *https://* to encrypt the data to and from the end points.

ENCRYPTION AT REST

Data at rest refers to data that is not moving, data on a drive, or backed up data. For example, this may be a file from a customer. Our internal policies restrict us from putting any client data on a laptop, or USB, or personal devices. Client data can only be accessed through the secure server. Any backed up data is encrypted and cannot be accessed without being restored to the data center.

STAFF TRAINING RELATED TO THE LAW(S)

Staff is instructed and trained to not store, remove, or share any customer data. We only use the customer's information in training the customer at the customer's site. Staff is trained on HIPAA Privacy, Security Rules, GLBA, which talks about safeguard procedures against fraud or identity theft and instruction about computer security, and FISMA (Federal Information and

Security). We also comply with FERPA, which includes hiring contractors to minimize security risks. Every employee and contractor is required to sign a confidentiality agreement as part of their employment package.

BREACH PLAN AND NOTIFICATION PROCESS

Our IT security company WLS monitors the servers for Security related Breaches. We require immediate Notification of any security breach so we can in turn immediately notify our clients that a breach has occurred, and what was breached. We have, to this date not had any security breach.

PROCESS AND POLICY TO RESTRICT DATA ACCESS TO ONLY THOSE WITH EDUCATIONAL INTEREST

The login and security policies within the program restrict access to the data to individuals that need access to the data. The district will specify to us who is allowed to access the information in the programs. The district also has the ability to change the level of access individuals have within the programs. Normal access is program dependent, e.g. teachers see own students, principals their building, etc. Educational Vistas can also use secure LDAP to allow the district's active directory server to provide an additional restriction on top of the security the programs provide.

DATA DISCLOSURE (STATEMENT OF USE)

Educational Vistas does not use client data. Client data is the property of the client. We do not share client information or client data with anyone. In our services to client district, we use client data within the programs for many reasons. Examples would be: To show a teacher which students missed specific standards, print student answer sheets for assessments, build Teacher SLOs, spin assessment data by student for use for teacher driven professional learning, use disaggregated data to set target scores for the district, for the districts to do state reporting like the Civil rights reports, VADIRS, DASA, Discipline Reporting, parent communication templates or to assist setting initial RTI goals based on assessment scores.

DATA RETURN OR DESTRUCTION UPON END OF CONTRACT OR CONTRACT TERMINATION

Educational Vistas will remove all customer data from our servers after receiving a written request from the customer to do so. We will also allow the customer to download extracts of the data before we remove it.

SECURITY PROTOCOLS RELATED TO ANY SUBCONTRACTORS

Subcontractors are required to adhere to the same level of security as our internal staff. We require contractors to sign documents stating they will safeguard the data and not use or share any of the district's data.

ABILITY TO CHALLENGE DATA ACCURACY

Much of the data we house comes from outside systems such as the district's Student Information System (SIS). We do have the ability to validate data on import to our system(s) and send email notifications to someone at the district that data may be missing that could cause inaccurate reporting to occur. Our Data Sync tool does this automatically if the district wants it. In the StaffTrac APPR system, where evidence can be entered by multiple users, the district can turn on the ability for the data to be user-, time-, and date-stamped. In the SafeSchoolsNY program, the system tracks who reported and who recorded each incident. The district also has the ability to change their own information in order to correct anything that is not accurate. We make it our priority to ensure data accuracy within the programs.

LUKAS J. CROWDER - CFO
(Authorized Representative)

(Signature)