Terms and Conditions for Data Privacy Policy

Union Public Schools

1) Use of, Storage of, or Access to, District Data

Contractor shall only use, store, or access District Data:

A) In accordance with, and only to the extent permissible under this Agreement; and

B) In full compliance with any and all applicable laws and regulations, only to the extent applicable to Contractor, but without limitation: Family Educational Rights and Privacy Act (FERPA), General Data Protection Rights (GDPR) and, Health Insurance Portability and Accountability Act (HIPAA), and any other applicable State or Federal law.

C) Any transmission, transportation, or storage of District Data outside the United States is prohibited except on prior written authorization by the District.

2) Safeguarding District Data

A) Contractor agrees that use, storage, and access to District Data shall be performed with that degree of skill, care, and judgment customarily accepted as sound, quality, and professional practices.

B) Contractor shall implement and maintain safeguards necessary to ensure the confidentiality, availability, and integrity of District Data.

C) Contractor shall implement and maintain any safeguards required to be implemented by applicable state and federal laws and regulations. Such safeguards shall include as appropriate, and without limitation, the following:

D) System Security. A System that is owned or operated by Contractor and contains District Data shall be secured as follows:

i) Contractor shall implement controls reasonably necessary to prevent a breach.

ii) The System shall use secure protocols and minimum 128 bit encryption to safeguard District Data in transit.

iii) Contractor understands the System may be placed on a public network and shall implement safeguards reasonably necessary to protect its system from compromises and attacks.

iv) Contractor will protect the system with properly configured and updated firewalls.

V) Contractor shall:

(1) Limit administrative access to the System.

(2) Limit remote access to the System.

(3) Limit account access and privileges to the least necessary for the proper functioning of the System.

(4) Remove or disable applications and services that are not necessary for the proper functioning of the System,

(5) Use named user accounts and not generic or shared accounts.

(6) Use Federated Single Sign On, Kerberos, or other industry compliant services for authentication and authorization.

(7) Enable an appropriate level of auditing and logging for the operating system and applications.

E) Product Maintenance and Support

i) Contractor shall have a process for the timely review, testing, and installation of patches essential for safeguarding the confidentiality, integrity, or availability of the System or District Data.

ii) Documented change management procedures shall be followed.

iii) Contractor shall ensure that the product is supported, provided that District maintains the requisite subscriptions. Contractor shall provide District with notice 12 months before the product becomes unsupported.

F) Contractor access to District systems

i) District login credentials may be given to contractors requiring access to secured computer equipment located on-site at the District for the purposes of scheduled troubleshooting, maintenance, or updates to software provided or supplied by Contractor and installed on District-owned computer equipment.

ii) If necessary and where appropriate, the District will provide the Contractor with credentials for logging in locally or through our secured Virtual Private Network (VPN).

iii) In order to establish a district login or a VPN account, a request must be made directly to the Executive Director of Technology stating:

(1) The security level of access needed

(2) The duration access must be granted

(3) Specific internal resources needed

iv) Passwords will follow industry standards for complex password structure as well as a minimum of 180 day password expirations.

v) As a condition of the Contractor's access to District computing equipment the Contractor represents that they will not attempt to access any system(s) other than the one(s) designated in the initial request nor will the Contractor use any computer equipment for any purpose that is unlawful.

G) All work performed by the Contractor while connected to District computing equipment is subject to monitoring by District staff.

3) Oversight

A) The District reserves the right to request security information reasonably necessary to ascertain District's own compliance with state and federal data privacy laws. Upon the District's request, Contractor shall provide a copy of its most recent third party report and that of any data center in which District's Data is stored.

4) Data Breach

A) If contractor suspects or becomes aware that District Data may have been accessed, disclosed, or acquired without proper authorization and contrary to the terms of this Agreement or the Contract, Contractor shall alert the District of any Data Breach within two business days, and shall immediately take such actions as may be necessary to preserve forensic evidence and eliminate the cause of the Data Breach.

B) Contractor shall give highest priority to immediately correcting any Data Breach and shall devote such resources as may be required to accomplish that goal. Contractor shall provide the District information necessary to enable the District to fully understand the nature and scope of the Data Breach.

C) Contractor shall provide notice and credit monitoring to parties affected by any Data Breach as required by law.

D) Contractor shall provide District information about what Contractor has done or plans to do to mitigate any deleterious effect of the unauthorized use or disclosure of, or access to, District Data.

E) If any work needs to be completed in order to resolve any breach issue and restore service, the District shall not be held liable or required to pay any additional money outside of the originally approved scope.

F) The District may discontinue any services or products provided by Contractor until the District, in its sole discretion, determines that the cause of the Data Breach has been sufficiently mitigated.

5) Data Scrubbing/Purging

A) In compliance with GDPR, if a student makes a request to purge all personal records, Contractor agrees to remove all personally identifiable information including text files, database records, and images.

6) Children's Online Privacy Protection Act (COPPA)

A) If contractor is going to collect personally identifiable information for any student under thirteen years of age, Contractor will comply with all requirements stated forth in COPPA.

7) No Surreptitious Code

Contractor warrants that, to the best of its knowledge, the System is free of and does not contain any code or mechanism that collects personal information or asserts control of the System without District's consent, or which may restrict District's access to or use of District Data. Contractor further warrants that it will not knowingly introduce, via any means, spyware, adware, ransomware, rootkit, key logger, virus, Trojan, worm, or other code or mechanism designed to permit unauthorized access to District Data, or which may restrict District's access to or use of District Data.

8) Compelled Disclosure

A) If Contractor is served with any subpoena, discovery request, court order, or other legal request or command that calls for disclosure of any District Data, Contractor shall promptly notify the District in writing and provide the District sufficient time to obtain a court order or take any other action the District deems necessary to prevent disclosure or otherwise protect District Data.

B) Contractor shall provide District prompt and full assistance in District's efforts to protect District Data. Where Contractor is prohibited by law from notifying the District of a legal request for District Data, Contractor will comply with all applicable laws and regulations with respect to the requested District Data.

9) Termination Procedures

A) Upon expiration or termination of the contract or project, contractor shall ensure that no data breach occurs and shall follow the District's instructions as to the preservation, transfer, or destruction of District Data.

B) The method of destruction shall be accomplished by "purging" or "physical destruction", in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88. Upon request by the District, Contractor shall certify in writing to District that return or destruction of data has been completed. Prior to such return or destruction, Contractor shall continue to protect District Data in accordance with this Agreement.

10) Survival; Order of Precedence

A) This Agreement shall survive the expiration or earlier termination of the Contract up to the point of all district data has been destroyed as defined in section 10 of this agreement. However, upon expiration or termination of the Contract, either party may terminate this Agreement. In the event the provisions of this Agreement conflict with any provision of the Contract, or Contractors' warranties, support contract, or service level agreement, the provisions of this Agreement shall prevail.

11) Definitions

Contractor: Any third party organization that will receive District data electronically via ftp, email, USB storage device, or in any electronic format as part of a business agreement, research project, or any other application where data is processed or stored.

District Data: District Data is any and all data that the District has disclosed to Contractor. For the purposes of this Agreement, District Data does not cease to be District Data solely because it is transferred or transmitted beyond the District's immediate possession, custody, or control.

Data Breach: The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of confidential or sensitive personal information maintained by the District as part of a database of personal information regarding multiple individuals and that causes or the District reasonably believes has caused or will cause loss or injury to any District constituent.

System: An assembly of components that supports an operational role or accomplishes a specific objective. This may include a discrete set of information resources (network, server, computer, software, application, operating system or storage devices) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Change Management: A formal process used to ensure that changes to a system are introduced in a controlled and coordinated manner. This reduces the possibility that unnecessary changes will be introduced to a system, that faults or vulnerabilities are introduced to the system, or that changes made by other users are undone.

Contract. Shall mean Contractors terms and conditions of sale and service.