Data Security and Privacy Addendum

A. Standard of Care

1. Provider acknowledges and agrees that, in the course of its Contract with Kids Hope Alliance (KHA), Provider may, directly or indirectly, receive or have access to Personal Identifiable Information (PII) that is protected under a variety of regulations including, but not limited to, the Family Educational Rights and Privacy Act (FERPA), Student Online Personal Information Protection Act (Florida SOPIPA), Health Insurance Portability and Accountability Act (HIPAA), and other applicable data privacy laws.

In general, PII is defined as any information or data that may identify an individual, such as the first name, last name (or combination of first initial and last name in combination with any of the following:

i. Home address, telephone number, email address, date of birth, or age;
ii. Government-issued identification numbers, such as social security number, driver's license number, state-issued identification number, passport number, alien registration number (A-Number), tax identification number (TIN) or military identification number;
iii. Financial account numbers, such as credit card number, debit card number, or credit report information. This includes any accompanying security codes, access codes, personal identification numbers (PINs), or passwords that could grant access to an individual's financial accounts;
iv. Biometric or health information, along with any additional data protected under HIPAA, such as medical records, insurance policy numbers, biometric identifiers (e.g. fingerprints, iris scans, or genetic data), diagnoses, treatment information, or any other broader category of health information that can be linked to an individual.
v. In combination with any data stated above, any educational information and PII specifically protected by FERPA, such as student's name, address, social security number, or student ID number. Additionally, any education or academic records which include documents, files, and other materials containing information directly related to a student and maintained by an educational agency or institution. Student data examples covered under FERPA include, but are not limited to, grades, transcripts, exam scores, attendance records, class rosters, disciplinary records, special education data, food program records, student photos, or specific personal characteristics, such as gender, ethnicity, date of birth, and religious information.

Notwithstanding the foregoing, PII shall not constitute information:

i. about an individual that has been made publicly available by a federal, state, or local governmental entity; or
ii. that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or which otherwise renders the information unusable.

Provider shall comply with the terms and conditions set forth in this Contract in its collection, receipt, transmission, storage, disposal, use and disclosure of such PII, and shall be responsible for the unauthorized collection, receipt, transmission, access, storage, disposal, use and disclosure of PII under its control or in its possession.

Furthermore, Provider shall be responsible for the actions and omissions of its employees and subcontractors who are authorized to access PII for obligations under this Contract (Authorized Persons) as if they were Provider's own actions and omission. Prior to being given access to PII, Provider shall ensure that Authorized Persons are bound in writing by confidentiality obligations to protect PII in accordance with the terms and conditions of this Contract.

2. All data collected on behalf of Kids Hope Alliance is deemed to be property of Kids Hope Alliance and is not property of Provider.

3. In recognition of the foregoing, Provider agrees and covenants that it shall:

i. Keep and maintain all such PII strictly confidential.
ii. Use and disclose PII solely and exclusively for the purposes for which the PII, or access to it, is provided pursuant to the terms and conditions of this Contract, and shall not divulge, communicate, use, sell, rent, transfer, distribute, or otherwise disclose or make available PII for Provider's own purposes or for the benefit of anyone other than Kids Hope Alliance, without KHA's prior written consent, which may be withheld at KHA's sole and absolute discretion.
iii. Not disclose PII to an Unauthorized Third Party, directly or indirectly, without express written consent from KHA, which may be withheld at its sole and absolute discretion. An Unauthorized Third Party is any person other than an Authorized Person. If any person or authority makes a demand on Provider purporting to legally compel it to divulge any PII, Provider shall:
    a. Immediately notify KHA of the demand before such disclosure so that KHA may first assess whether to challenge the demand prior to Provider's divulging of such PII;
    b. Be responsible to KHA for the actions and omissions of such Unauthorized Third Party concerning the treatment of such PII as if they were Provider's own actions and omissions; and
    c. Require the Unauthorized Third Party that has access to PII to execute a written Contract agreeing to comply with the terms and conditions of this Contract relating to the treatment of PII. Provider shall not divulge such PII until KHA either has concluded not to challenge the demand, or has exhausted its challenge, including appeals, if any.

B. Personal Identifiable Information Security

Provider shall protect and secure data in electronic form containing such PII.

At a minimum, Provider's safeguards for the protection of PII shall include:

i. Encrypting, securing or modifying such PII by any method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.
ii. Limiting access of PII to Authorized Persons.
iii. Implementing network, device, application, database, and platform security.
iv. Securing business facilities, data centers, paper files, servers, back-up systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability.
v. During the term of each Authorized Person's employment by Provider, Provider shall, at all times, cause such Authorized Persons to abide strictly by Provider's obligations under this Contract. Provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of PII by any of Provider's officers, directors, partners, principals, employees, agents, contractors, or vendors. Upon KHA's request, Provider shall promptly identify all Authorized Persons as of the date of such request to KHA in writing.

vi. All Providers must:
    a. Appoint a cyber security point person with accountability for agency cyber security.
    b. Implement multifactor authentication (MFA) for access to email and platforms containing PII.
    c. Maintain an inventory of all hardware, software, databases, and applications used to store, process or transmit PII.
    d. Implement least privilege access principles for all systems or applications with access to PII.
    e. Regularly review permissions to PII and update user access permissions.
    f. Only allow users to access systems containing PII through the use of "named" accounts. A named account is one that is assigned and traceable to a specific person.
    g. Do not allow users to access PII through shared or generic accounts that are used amongst multiple individuals.
    h. Change default passwords to systems that store, process, or transmit PII.
    i. Enforce a minimum password strength of 12 characters on systems containing PII.
    j. Train employees on the importance of PII security.
    k. Ensure that credentials of departing employees are revoked by the end of the day of their day of departure, if not sooner.
    l. Encrypt PII stored on any mobile media, mobile devices, and portable computing devices such as laptops.
    m. Ensure that administrative accounts are separated from standard user accounts.
    n. Implement account lockout after a specific number of consecutive, unsuccessful login attempts in a short period of time (e.g. 5 failed attempts over 2 minutes)
    o. Regularly patch all assets that store, process, or transmit PII.

p. Maintain physical security of printed PII materials (e.g. locked filing cabinets, etc.)
q. Maintain physical security of assets that store, process, or transmit PII- (e.g. do not leave laptops unattended), and establish a remote work policy that ensures users are safely handling their work devices offsite.
r. Maintain secure information transmission, storage, and disposal; implementing authentication and access controls within media, applications, operating systems and equipment.
s. Provider shall dispose, or arrange for the disposal, of customer records that contain PII within its custody or control when the records are no longer required to be retained. Such disposal shall involve shredding, erasing or otherwise modifying PII in its control or possession to make it unreadable or undecipherable.

vii. It is recommended that providers-

a. Implement "phishing resistant" MFA, meaning a push notification with a number match or hardware token such as a Yubikey. An MFA code sent via SMS (text message) or voice should only be used when no other options are technically possible.
b. Conduct ongoing general cybersecurity training. Training must include social engineering training, security best practice training, insider threat training, and simulated social engineering tests.
c. Ensure sensitive data, including credentials are not stored in plaintext (e.g. an Excel document named "passwords"). Ensure credentials are stored in a secure manner such as a password manager.
d. Ensure users are using unique and separate credentials for accessing systems containing PII, unless Single Sign On is used.
e. Implement Endpoint Detect and Response (EDR) software on all endpoints that store, process, or transmit PII and all endpoints that provide security (domain controllers, servers, etc.) to the information system.
f. Implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law, as required by KHA from time to time.
g. Purchasing and maintaining cyber insurance coverage, in accordance with Section 4.6, paragraph 8 and Attachment G of the RFP.

C. Security Breach Procedures

For purposes of this Contract, "Security Breach" is defined as unauthorized access of data in electronic form containing PII, or a breach or alleged breach of this Contract relating to such privacy practices. Good faith access of PII by an employee or agent of the covered entity shall not constitute a breach of security under this Contract, so long as the information is not used for a purpose unrelated to the business of KHA, or as a result of any other unauthorized use. **In the event of a Security Breach, Provider shall:**

1. Notify KHA immediately, but not later than forty-eight (48) hours, after Provider becomes aware of it by emailing KHA with a read receipt at KHADataSecure@coj.net ; and with a copy of such email to Provider's program manager at KHA. The notice shall include, at a minimum:

i. the date, estimated date, or estimated date range of the Security Breach; and
ii. a description of the PII that was accessed or reasonably believed to have been accessed as a part of the Security Breach.
iii. In the event email is compromised or otherwise not available, a report can be filed by calling, 904-255-4410.

2. To the extent legally permissible, confer with KHA prior to informing any third party of any Security Breach related to this Contract. Provider and KHA shall communicate regarding:

i. whether notice of the Security Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law regulation, or otherwise; and
ii. the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.

3. Take steps to immediately remedy any Security Breach and prevent any further Security Breaches from happening. Provider shall undertake all remediation action at their own expense. All of Provider's incident response and security remediation efforts shall be executed in accordance with applicable privacy rights, laws, regulations and standards, or as otherwise required by KHA at its sole and absolute discretion.

Provider shall be solely responsible for all costs associated with a Security Breach. KHA may seek to recover any costs it expends as a result of such Security Breach from Provider.