PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

SCIO CENTRAL SCHOOL DISTRICT is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, SCIO CENTRAL SCHOOL DISTRICT informs the school community of the following:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by New York State is available for public review at the following website http://www.nysed.gov/data-privacy-security/student-data-inventory or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.

5. Parents have the right to submit complaints about possible breaches of student data addressed. Complaints should be directed in writing to SCIO CENTRAL SCHOOL DISTRICT Data Privacy Officer, 3968 Washington Street Scio, NY 14880 or by using the form available at the following website: https://caboces.org/resources/new-york-state-education-law-2d/report-an-improper-disclosure/. Complaints may also be directed in writing to Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234 or by using the form available at the following website: http://www.nysed.gov/data-privacy-security/report-improper-disclosure

IN WITNESS WHEREOF, the parties hereto have executed this agreement as of the day and year first written above.

Authorized Vendor Signature

9-21-2020
Date

Authorized SCIO CENTRAL SCHOOL DISTRICT Signature

9/24/2020
Date

VENDOR INFORMATION REGARDING DATA PRIVACY AND SECURITY

Vendor: Buncee LLC

Product: Buncee Classroom
Buncee for Schools & Districts

Collects: ☒ Student Data ☒ Teacher or Principal Data □ Does not collect either

Educational agencies including Cattaraugus-Allegany-Erie-Wyoming BOCES are required to *post information about third-party contracts on the agency's website* with the Parents Bill of Rights. To that end, please complete the table below with information relevant to NYS Education Law 2-d and Part 121.3 of the Commissioner's Regulations. Note that this applies to all software applications and to mobile applications ("apps").

Part 1: Exclusive Purposes for Data Use

The exclusive purposes for which the student data (or teacher or principal data) will be used by the third-party contractor:

The exclusive purposes for which the student data (or teacher or principal data) will be used by the third-party contractor:
The purpose of data processing is to allow Buncee to provide the requested Services to the District and perform the obligations under our Agreement. More specifically, the purpose of processing data is to enable school oversight and ensure appropriate structure and interaction within a school account on buncee.com. The processing of data enables the interaction, communication, creation and sharing within the classroom/school/district account; allows educators and/or administrators to monitor accounts, set permissions and deliver educational content; allows educators to differentiate and personalize a student's educational experience; and provides the admin-educator-student hierarchy within the account. Buncee requires data capture and use for the following reasons:

- **To confirm the identity of students and educators/administrators**
- **To provide educational services and content**
- **To allow subscribers to create and manage classes, personalize and differentiate instruction, and monitor and assess student progress**
- **To allow subscribers to monitor and safeguard student welfare**
- **To allow subscribers to set creation and sharing permissions and privacies schoolwide**
- **To inform existing subscribers about feature updates, site maintenance, and programs/initiatives (does not include subaccounts)**

Part 2: Subcontractor Oversight Details – Select the appropriate option below.

□ This contract has no subcontractors.

☒ This contract has subcontractors. As such, the third-party contractor will take the following steps to ensure that any subcontractors, assignees, or other agents who see, or receive, this protected data are contractually required to obey the same data protection and security requirements that the third-party contractor is required to obey under state and federal law:
Buncee shall enter into a written agreement with any Subcontractors requiring the Subcontractor to uphold data protection practices that protect the District Data to the standard required by the Data Protection Laws (NYSED Law 2-D).

Part 3: Contract Lifecycle Practices

The contract expires on 08/31/2021 unless renewed or automatically extended for a term pursuant to the agreement. When the contract expires, protected data will be deleted by the contractor, via shredding, returning of data, mass deletion, and upon request, may be exported for use by Sa before deletion.

Part 4: Student Educational Records / Improper Disclosure

A. For information on FERPA (Family Educational Rights and Privacy Act), which is the federal law that protects the privacy of student education records, visit the U.S. Department of Education FERPA website.

B. A complaint or report of improper disclosure may be completed by submitting the Improper Disclosure Report form.

Part 5: Security Practices

A. Protected data provided to the contractor will be stored: (include *where* and *how*)

The following preemptive safeguards are in place to identify potential threats, manage vulnerabilities and prevent intrusion:

- **All security patches are applied routinely**
- **Server access logging is enabled on all servers**
- **Fail2ban (an intrusion prevention software framework that protects servers from brute-force attacks) is installed on all servers and will automatically respond to illegitimate access attempts without intervention from Buncee's engineers**
- **Publicly accessible parameter for database instances is set to No, thereby disallowing any unauthorized access to the database servers**
- **SSH key-based authentication is configured on all servers**

Buncee serves 100% of its traffic over HTTPS. The HTTPS you see in the URL of your browser means when you go to buncee.com, you're guaranteed to be getting the genuine Buncee website. With HTTPS in place, all interactions with Buncee will be undecipherable by an outside observer. They are unable to read or decode data. HTTPS is the same system that many sensitive websites, like banks, use to secure their traffic. This applies to all our custom Buncee for Schools & Districts urls too.

Buncee uses SSL security at the network level to ensure all information is transmitted securely. All content (i.e., photos, video, audio, and other content added to your Buncees) is encrypted at rest. All passwords are encrypted using bcrypt algorithm which is based on the secure blowfish encryption algorithm.

Account information is stored in access-controlled data centers operated by industry leading partners with years of experience in large-scale data centers. All user information is stored redundantly and backed up in geographically distributed data centers. We utilize multiple distributed servers to ensure high levels of uptime and to ensure that we can restore availability and access to personal data in a timely manner.

Buncee's application is hosted on cloud servers managed by Amazon Web Services and Digital Ocean, both of whom have rigorous physical measures to safeguard data, and are compliant with security standards including ISO 27001, SOC 2, PCI DSS Level 1, and FISMA. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. These data centers are staffed 24/7/365 with onsite security to protect against unauthorized entry. Each site has security cameras that monitor both the facility premises as well as each area of the datacenter internally. There are biometric readers for access as well as at least two factor authentication to gain access to the building. Each facility is unmarked so as not to draw any additional attention from the outside and adheres to strict local and federal government standards. Furthermore, physical access to our servers would not allow access to the actual data, as it is all protected via encryption.

B. The security protections taken to ensure data will be protected that align with the NIST Cybersecurity Framework and industry best practices include:

Please see Buncee's attached Data Privacy Plan.

Part 6: Encryption Practices

☒By checking this box, contractor certifies that data encryption is applied in accordance with NYS Education Law Section 2-d 5(f)(5).