Addendum "A"
DATA PRIVACY PLAN AND
PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

Pursuant to Section 2-d of the Education Law, agreements entered between the District and a third-party contractor which require the disclosure of student data and/or teacher or principal data that contains personally identifiable information ("**PII**") to the contractor, must include a data security and privacy plan and must ensure that all contracts with third-party contractors incorporate the District's Parents' Bill of Rights for Data Security and Privacy.

As such, Hackersjack ("**Contractor**") agrees that the following terms shall be incorporated into the contract for services ("**the Contract**") and it shall adhere to the following:

1. The Contactor's storage, use and transmission of student and teacher/principal PII shall be consistent with the District's Data Security and Privacy Policy available here: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.capitalregionboces.org/wp-content/uploads/2023/05/5676-CRB-Privacy-and-Security-for-StudentTeacher-and-Principal-Data-Policy-3-30-20.pdf

2. Contractor shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.

3. The exclusive purposes for which the student data or teacher or principal data will be used under the contract are set forth in Paragraph 2 of the Contract only for the term of the Contract as set forth in Paragraph 1.

4. The Contract shall maintain the following administrative, operational and technical safeguards and practices in place to protect PII, which shall align with the NIST Cybersecurity Framework, including:

    a. PII data will be protected using encryption while in motion and at rest by using industry-standard security measures, including encryption protocols that comply with New York law and regulations to preserve and protect PII data.

    b. PII will be stored in a manner as to protect its security and to mitigate any potential security risks. Specifically, all student data and/or teacher or principal data will be stored on the Amazon Web Services secured cloud within the United States. The security of this data will be ensured by the use of encryption protocols.

5. The Contractor shall ensure that no PII is disclosed to employees, subcontractors, or other persons or entities unless they have a legitimate educational interest and only for purposes necessary to provide services under the Contract.

    a. By initialing here _____ Contractor represents that it will not utilize any subcontractors or outside entities to provide services under the Contract and shall not disclose any PII other than as required pursuant to paragraph 6 below.

6. Contractor shall ensure that all employees, subcontractors, or other persons or entities who have access to PII will abide by all applicable data protection and security requirements, including, but not limited to those outlined in applicable laws and regulations (e.g., FERPA, Education Law Section 2-d). Contractor shall provide training to any employees, subcontractors, or other persons or entities to whom it discloses PII as follows: Training has been scheduled to be conducted in each quarter, focusing on PII protection and awareness methods to enhance employees' knowledge of existing and emerging threats in the areas of identity theft and data privacy, and the most current best practices for securing and protecting PII. The objective of this training sessions is to build knowledge and skills that will enable staff to protect PII and comply with the laws and regulations of states and federal government.

7. Contractor shall not disclose PII to any other party other than those set forth in paragraph 4 above without prior written parental consent or unless required by law or court order. If disclosure of PII is required by law or court order, the Contractor shall notify the New York State Education Department and the District no later than the time the PII is disclosed unless such notice is expressly prohibited by law or the court order.

8. Upon expiration of the contract, the PII will be returned to the District and/or destroyed. Specifically, once the contract period is completed, Contractor will not retain or process any information containing PII information. All PII data will be deleted/erased from all servers where data has been stored and hosted. Contractor will provide a statement to the District confirming the destruction of the data and method used.

9. The parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data collected in accordance with the procedures set forth in the FERPA regulations at 99 C.F.R. Part 34, Subpart C, §§99.20-99.22.

10. The Contractor shall take the following steps to identify breaches or unauthorized releases of PII and to notify the District upon learning of an unauthorized release of PII.

    a. Provide prompt notification to the District no later than seven (7) calendar days from date of discovery of a breach or unauthorized release of PII. Contractor shall provide notification to the District's data privacy officer by phone and by email prior to providing any notice of the incident directly to any other BOCES or affected Participating Educational Agency.

b. Contractor shall cooperate with the District and law enforcement to protect the integrity of the investigation of any breach or unauthorized release of PII.

c. Where a breach or unauthorized release is attributed to the Contractor, the Contractor shall pay for or promptly reimburse the District for the full cost of such notification.

11. A complete list of all student data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, or parents may obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.

12. Parents have the right to file complaints with the District about possible privacy breaches of student data by the District's third-party contractors or their employees, officers, or assignees, or with NYSED. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to CPO@mail.nysed.gov.

Contractor Signature: Brian J Bert

The District shall publish this contract addendum on its website.

Attachment "A"

PARENTS' BILL OF RIGHTS FOR STUDENT DATA PRIVACY AND SECURITY

Capital Region BOCES, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. BOCES establishes the following parental bill of rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.

- A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by BOCES or any a third party contractor. BOCES will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by BOCES in accordance with BOCES policy;

- Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see 5500-R);

- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. 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;

- A complete list of all student data elements collected by the State Education Department is available for public review at http://nysed.gov/data-privacy-security or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to the Data Protection Officer, (518) 464-5139, DPO@neric.org, Capital Region BOCES, 900 Watervliet-Shaker Rd., Albany NY 12205. Complaints can also be directed to the New York State Education Department online at http://nysed.gov/data-privacy-security by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@mail.nysed.gov or by telephone at 518-474-0937.

- Parents have the right to be notified in accordance to applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

- Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.

- In the event that BOCES engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting the Data Protection Officer, (518)-464-5139, DPO@neric.org, 900 Watervliet-Shaker Rd., Albany NY 12205, or can access the information on BOCES' website https://www.capitalregionboces.org/.

Attachment B

Privacy Policy – Hackersjack, INC.

Effective and Last Reviewed: **June 6, 2023**

Hackersjack offers a cloud-based online learning platform that provides a knowledge hub for kids to learn to respect cyber security in a fun and safe environment. We partner with schools to provide the opportunity to incorporate these critical life skills into a school curriculum. This privacy policy explains what information we may collect about you when you visit our website hackersjack.com (our "Website") or when you use our platform (our "Platform") (together our "Services"). We reserve the right to change this privacy policy. When we do so, we will update the "Effective and Last Reviewed Date" listed above. Your continued use of our Services after that date indicates your consent to those changes.

Collection of your personal information

In order to use our Platform, we need to collect some information from and about you.

If you are a school teacher, we will collect information from you in order to set up your Hackersjack classroom account. This includes your name, contact information, username and credentials to access the platform, the name of the school where you teach, the grade level you teach and the number of kids in your class.

To allow students in your class to access the Platform, a school or school district official will need to provide us with some information about the participating students. To set up a student account, we may need the student's name, school assigned id number, grade level, class information and school email address. We will also collect student demographic information to ensure our Platform is reaching all demographics within a school community.

To follow your learning progress, we will collect information about what lessons are completed and the results of any assessments. We may also ask students to complete a survey to learn about their experience with our Platform.

When you visit our Website, we collect certain information automatically through cookies and other technologies. This includes your Internet Protocol ("IP") address, the pages you visit, your browser, operating system and access dates and times. We use this information to improve, monitor, analyze your use of and administer our website.

Use of your personal information

We use the information we collect from you to provide our Services and for the following purposes:

- To offer our Platform and full functionality of the Platform, including the ability to create accounts on our Platform, access and participate in lessons on the Platform along with tracking progress and scores on assessments.
- To improve our Services, develop new offerings and perform analytics.
- To confirm our Services are effectively reaching all demographics.
- To send administrative messages about your use of the Platform, including technical notices, updates, and support messages.
- To send you information about your use of the Platform.
- Consistent with our obligations under the Family Educational Rights and Privacy Act (FERPA), we will use "personally identifiable information" from "education records," as those terms are defined in FERPA, as directed by the school or district for their educational purposes.
- To offer our Website and its information and services.
- To manage our relationship with you, including respond to messages and questions.
- To notify you of any changes to our Services.
- To enforce our Terms of Service, Privacy Policy and any licensing agreements.
- We may use and retain aggregated, de-identified information to develop and improve our educational products, to demonstrate the efficacy of our products, including in the marketing of our products.

Sharing of your personal information

To provide you with full optimization of the Services, we may need to share your information as described below:

- Information associated with classroom accounts will be shared with the school or school district official that set up the account. These accounts may also be shared with other individuals at the school that are authorized to access these accounts.
- We use service providers to help us operate our Services and provide us with certain analytics and other services. We hold our service providers to confidentiality and privacy obligations in relation to the protection of your personal information.
- Authorized law enforcement, regulatory or government agencies, courts or third parties where we reasonably believe that such disclosure is required under

applicable law, to establish or defend our legal rights, or to protect your safety or the safety of others using our Services.
- In the event of a reorganization, merger, sale, bankruptcy or other business change, we may need to share your information.

We do not sell your information or share it with third-parties for advertising purposes.

Children's Privacy

Currently, the Hackersjack Platform is offered only to schools, school districts and other educational or learning institutions. We comply with FERPA and relevant state laws concerning the privacy of students. We do not collect information from a child until we have obtained the required consent. Schools that use our Platform as an educational tool may create a classroom account and provide consent for us to collect personal information from the student.

We only collect the amount of information needed to provide the service.

Access

If you would like to review, correct, update or request that we delete personal information you or your students have provided to us, you may do so by contacting us using the contact information below.

Third-Party Links

Our Services may contain links to other websites. We are not responsible for the content or privacy practices of these linked websites. We encourage you to review the privacy policies posted on these sites before providing any personal information.

Security

We have taken appropriate security measures to safeguard your personal data by implementing reasonable technical and physical security measures based on the type of data we process.

Retention

For Platform users, we retain your information for as long as you have an account with us. After a period of inactivity, we will deactivate your account and delete your personal information. You may contact us to request that we delete your account using the

contact information below. We may de-identify information for analytics purposes. De-identified information will be retained indefinitely.

Do Not Track

Our Website does not respond to do-not-track signals.

Contacting us

HackersJack welcomes your comments regarding this Privacy Policy. If you have any questions about this Privacy Policy and would like further information, please contact us via schools@hackersjack.com.

Hackersjack, Inc.
1015 15th Street, NW, Suite 600
Washington D.C., 20005
www.hackersjack.com