NEW YORK STATE MODEL DATA PRIVACY AGREEMENT
FOR EDUCATIONAL AGENCIES

Olean City School District

and

Zaner-Bloser, Inc.

This Data Privacy Agreement ("DPA") is by and between the Olean City School District ("EA"), an Educational Agency, and Zaner-Bloser, Inc. ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose**: To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Educational Agency**: As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable

form in which there is a low probability of assigning meaning without use of a confidential process or key.

8. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. **Compliance with Law.**

   In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated 1/5/24 ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et

seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. **Authorized Use.**
   Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. **Data Security and Privacy Plan**.
   Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. **EA's Data Security and Privacy Policy**
   State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. **Right of Review and Audit.**
   Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. **Contractor's Employees and Subcontractors**.

(a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.

(b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

(c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.

(d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.

(e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. **Training**.

Contactor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. **Termination**

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. Data Return and Destruction of Data.

(a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.

(b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

(c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

(d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

(a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

Name:	***Marc Friends***
Title:	***Technology Coordinator/District Privacy Officer***
Address:	***410 West Sullivan Street***
City, State, Zip:	***Olean, NY 14760***
Email:	***DPO@oleanschools.org***

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. **Notification to Individuals.**

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. **Termination**.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. **Parent and Eligible Student Access**.

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. **Bill of Rights for Data Privacy and Security**.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. **Priority of Agreements and Precedence.**

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. **Execution.**

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

3. **Cyber Insurance.**

If the Vendor will be communicating with the District electronically and/or collecting any sensitive staff or student data, the Vendor must have coverage applicable to first- and third-party claims including but not limited to data compromise expenses and liability, forensic review costs, legal review costs, data restoration and re-creation costs, public relations costs, extortion costs, network security liability, identity recovery costs, regulatory fines and penalties, and credit monitoring costs. Coverage limits shall be no less than:

Each Occurrence/Claim	$1,000,000
Aggregate	$1,000,000

EDUCATIONAL AGENCY	**CONTRACTOR**
BY: *[Signature]*	BY:
Marc D Friends	***Robert Heighton***
Technology Coordinator/District Privacy Officer	VP, Operations
Date: 1-5-2024	Date: 1/5/2024

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA at: https://www.oleanschools.org/Page/8316, by email to DPO@oleanschools.org. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	
[Printed Name]	Robert Heighton
[Title]	VP, Operations
Date:	1/5/24

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	Zaner-Bloser, Inc.
Description of the purpose(s) for which Contractor will receive/access PII	Legitimate business purposes such as product improvement.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term	Contract Start Date 1/5/24___ Contract End Date _12/31/24_____
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ☒ Contractor will not utilize subcontractors. ☐ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary,

	the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☒ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Please see attached Privacy Policy, Technology Safeguards, and Data Breach Response Plan
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	
[Printed Name]	Robert Heighton
[Title]	VP, Operations
Date:	1/5/24

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state**. While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Please see attached Privacy Policy, Technology Safeguards, and Data Breach Response Plan, and Schedule of Data
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Please see attached Privacy Policy, Technology Safeguards, and Data Breach Response Plan, and Schedule of Data
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Please see attached Privacy Policy, Technology Safeguards, and Data Breach Response Plan, and Schedule of Data
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	Please see attached Privacy Policy, Technology Safeguards, and Data Breach Response Plan, and Schedule of Data
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Please see attached Privacy Policy, Technology Safeguards, and Data Breach Response Plan, and Schedule of Data
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Please see attached Privacy Policy, Technology Safeguards, and Data Breach Response Plan, and Schedule of Data
7	Describe your secure destruction practices and how certification will be provided to the EA.	Please see attached Privacy Policy, Technology Safeguards, and Data Breach Response Plan, and Schedule of Data
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Please see attached Privacy Policy, Technology Safeguards, and Data Breach Response Plan, and Schedule of Data
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

PRIVACY POLICY

Zaner Bloser, Inc. ("Zaner-Bloser", "we", "us") respects your privacy and is committed to protecting it through our compliance with this policy.

This policy was last updated on June 29, 2020.

For your convenience, here is our contact information:

Our postal address is
PO Box 16764
Columbus, OH 43216-6764

Our address is
1400 Goodale Boulevard, suite 200
Grandview Heights, OH 43212

We can be reached via e-mail at customerexperience@zaner-bloser.com or you can reach us by telephone at 1-800-421-3018.

MYZBPORTAL.COM

Please be advised that there are important differences in how Zaner-Bloser handles data in connection with the MYZBPORTAL as compared to our public-facing consumer websites, specifically in connection with any data that may include Student PII (Personally Identifiable Information).

School data and PII:

MyZBPortal.com collects the following student PII:

- Student first name (provided by district/school/institution)
- Student last name (provided by district/school/institution)
- Student ID (provided by district/school/institution)
- IP address
- Student score data (from completing online activities)

We only collect IP addresses for traffic and security monitoring purposes and delete these logs regularly (typically every other month). Schools can also request to delete these IP logs by submitting a request in writing to ZB Customer Experience.

- We do not sell student information.
- We do not target students with advertisements.
- We only request and use student personal information for legitimate business reasons.

Cookies:

Superkids Portal (Teachers, Admins, Parents) and Superkids Online Fun app and desktop shortcut (Students)
The entire site maintains cookies from the moment you visit the login page. The sole purpose of the use of cookies on the Superkids Portal is to track the user's session and visit. Zaner-Bloser, Inc.'s use of cookies is specifically limited to the legitimate business use for operation of the portal and cookies are never used for any targeted advertisements toward students.

ZB Portal (Teachers, Admins, Students)
The entire site maintains cookies from the moment you visit the login page. The sole purpose of the use of cookies on the MYZBPortal is to track the user's session and visit. Zaner-Bloser, Inc.'s use of cookies is specifically limited to the legitimate business use for operation of the portal and cookies are never used for any targeted advertisements toward students.

Data encryption:

Stored data (i.e. data at rest) is stored securely on an encrypted drive. Data on backup storage is encrypted using AES 256-bit encryption. Data 'in-transit' is encrypted using well-known technologies such as "Secure Sockets Layer (SSL)" or "Transport Layer Security (TLS)". In-transit encryption is end-to-end from the client web browser through our cloud network. These protocols ensure privacy between communicating applications and their users on the Internet. When a server and client communicate, these technologies ensure that no third party may eavesdrop or tamper with any message.

Data retention:

At any time, an account administrator may request to purge school data (such as student and/or teacher information). This action will be performed by a ZB representative. School information will remain on backup storage for disaster recovery purposes for another 15 days, but thereafter will be removed completely from all storage devices. Schools can request to delete school data submitting a request in writing to ZB Customer Experience.

Data access:

Only authorized individuals are provided access to our systems. Passwords are never transmitted using insecure communication protocols. Access by Company's support personnel is based on "least privileged" and "need to know" basis. While some Company support personnel generate usage reports and have access to data for analytics, none of the resultant data contains Personally Identifiable Information (PII).

System hosting:

Our systems (servers and data) are currently hosted on dedicated machines in secured facilities at a third-party hosting provider located in the United States.

Perimeter security:

Firewalls and perimeter detection systems have been designed and deployed to help detect and prevent unauthorized access into our systems.

Vulnerabilities and patching:

We routinely scan our systems for vulnerabilities. The vulnerabilities are reviewed and addressed/patched as appropriate.

Consent from Schools regarding Students' Personal Information:

The Children's Online Privacy Protection Act ("COPPA") permits a school, acting in the role of "parent" to provide required consents regarding personal information of students who are under the age of 13. Where a school is the subscriber to our portal, we rely on this form of COPPA consent. We provide the school with this privacy policy, to ensure that the school, in providing its COPPA consent, has full information and assurance that our policies comply with COPPA.

The Family Educational Rights and Privacy Act ("FERPA") permits a school to provide educational records (including those that contain students' personal information) to certain service providers without requiring the school to obtain specific parental consent. FERPA permits this where the service provider acts as a type of "school official" by performing services, for example, that would otherwise be performed by the school's own employees. We fulfill FERPA requirements for qualifying as a school official by, among other steps, giving the school direct control with respect to the use and maintenance of the education records at issue (including associated personal information), and refraining from re-disclosing or using this personal information except for the purposes of providing this portal to the school. We comply with FERPA by relying on this form of consent.

Your Rights:

As a user of the portal, you have the rights to access, export, be informed about, rectify, object to the further processing of, restrict the processing of, withdraw consent to the processing of and erase your personal information. If you are a student at an educational institution using the Portal, you should direct any requests to exercise your data rights to the appropriate representative at your educational institution. If you are an educator or an administrator, you may reach out to us directly via e-mail at customerexperience@zaner-bloser.com or you can reach us by telephone at 1-800-421-3018.

TECHNOLOGY SAFEGUARDS – MYZBPORTAL.COM

School data and PII:

MyZBPortal.com collects the following student PII (personally identifiable information):

- Student first name (provided by district/school/institution)
- Student last name (provided by district/school/institution)
- Student ID (provided by district/school/institution)
- IP address
- Student score data (from completing online activities)

We only collect IP addresses for traffic and security monitoring purposes and delete these logs regularly (typically every other month). Schools can also request to delete these IP logs by submitting a request in writing to ZB Customer Experience.

- We do not sell student information.
- We do not target students with advertisements.
- We only request and use student personal information for legitimate business reasons.

Data encryption:

Stored data (i.e. data at rest) is stored securely on an encrypted drive. Data on backup storage is encrypted using AES 256-bit encryption. Data 'in-transit' is encrypted using well-known technologies such as "Secure Sockets Layer (SSL)" or "Transport Layer Security (TLS)". In-transit encryption is end-to-end from the client web browser through our cloud network. These protocols ensure privacy between communicating applications and their users on the Internet. When a server and client communicate, these technologies ensure that no third party may eavesdrop or tamper with any message.

Data retention:

At any time, an account administrator may request to purge school data (such as student and/or teacher information). This action will be performed by a ZB representative. School information will remain on backup storage for disaster recovery purposes for another 15 days, but thereafter will be removed completely from all storage devices. Schools can request to delete school data submitting a request in writing to ZB Customer Experience.

Data access:

Only authorized individuals are provided access to our systems. A username and password must be input and authenticated prior to gaining access to any information. Passwords use one-way salted hashes and technical support does not have access to a user's password. Passwords are **never** transmitted using insecure communication protocols. Access by Company's support personnel is based on "least privileged" and "need to know" basis. While some Company support personnel generate usage reports and have access to data for analytics, none of the resultant data contains Personally Identifiable Information (PII).

System hosting:

Our systems (servers and data) are currently hosted on dedicated machines in secured facilities at a third-party hosting provider located in the United States.

TECHNOLOGY SAFEGUARDS – MYZBPORTAL.COM

Perimeter security:

Firewalls and perimeter detection systems have been designed and deployed to help detect and prevent unauthorized access into our systems.

Vulnerabilities and patching:

We routinely scan our systems for vulnerabilities. The vulnerabilities are reviewed and addressed/patched as appropriate.

Technical Requirements for MyZBPortal.com

Note: for the best experience, we recommend keeping your browser updated to the latest version.

DEVICE

	Windows	Mac	Chromebook	iPad	Android tablet
CPU	Dual Core or higher			iPad 5 or newer	Quad-Core or higher
RAM	8GB	8GB	4GB	2GB	3GB
Resolution	1280x800 or higher				
Screen size	n/a			9" or larger	

OPERATING SYSTEM

	Windows	Mac	Chromebook	iPad	Android tablet
OS	Windows 10 or higher	MacOS v 11 (Big Sur) or higher	latest	iOS 13 or higher	10.0 or higher

Chromebooks: for your security, and to ensure that you can run our applications properly, we recommend that you use Chromebooks that have not reached Auto Update Expiration.

BROWSER

	Windows	Mac	Chromebook	iPad	Android tablet
Chrome	99 or higher	99 or higher	latest	99 or higher	99 or higher
Edge	98 or higher				
Safari	14 or higher			14 or higher	
FireFox	99 or higher	99 or higher			
Internet Explorer	*not supported*	n/a			

Superkids Online Fun

To use Superkids Online Fun on **an iPad or Android tablet device**, you must download the Superkids Online Fun app from the App Store or Google Play store. Superkids Online Fun is not playable through the browser on iPad or Android devices. To run the app successfully, ensure that your iPad or Android tablet device meets the device and operating system requirements above.

Additional requirements

- Cookies and JavaScript enabled
- PDF reader such as Adobe Acrobat
- Third-party add-ons disabled (browser add-ons can cause issues)
- HTTPS support enabled
- TLS 1.2 or higher

Network Connectivity

Bandwidth

A broadband internet connection is required. Size will vary depending on the number of concurrent users and content being accessed. We recommend a minimum of 5mb dedicated.

The minimum recommended average for each computer or device:

- 1mbps/workstation or greater recommended

Average, peak, and initial bandwidth requirements vary greatly depending on the product and the usage. No matter how fast the network connection between workstations and servers, if other bandwidth-intensive activities (VoIP, streaming video, audio downloads, database backups, etc.) are running on the network at the same time, performance may suffer. For this reason, the use of packet-shaping techniques on heavily trafficked networks is recommended.

Wireless

Zaner-Bloser software operates over TCP/IP networks including wireless (802.11.a, g, n). Refer to your wireless access point's manufacturer-recommended device limits.

Firewall & Content Filtering

If you employ a centralized content filtering mechanism in your network, this can impact content load times. You should disable content filtering from the following domains and IPs which are used to serve Zaner-Bloser online materials:

- 72.3.207.81
- *.myzbportal.com
- fast.wistia.net (streaming video content)
- zaner-bloser-zbportal.azureedge.net
- prod-zbportal.azurewebsites.net
- zb-portal.azureedge.net

Content is delivered over both HTTP & HTTPS protocols on ports 80 and 443, respectively, and your firewall must allow packet delivery over those ports from the domains listed above.

Zaner-Bloser, Inc. Security Incident Response Process

The following denotes the high-level steps to be followed when a potential security issue is suspected, reported, or detected. In case of an actual *security incident*, detailed procedures for each of the steps will be carried out based upon the type and/or nature of the incident.

Assessment

- Assess the potential security issue and all pertinent information to determine if the event is an actual security incident.

  Note: This process will stop here if it is determined that the reported issue was not an actual security incident and no breach occurred
- Determine if any *Cardholder Data* is involved
- Create a Security Incident Report Form and document the preliminary findings
- Notify (via email) SIRT at: SIRT@highlights.com and the Information Security Steering committee (ISSC) at: ISSC@Highlights.com that an actual security incident has occurred
- If necessary, notify the user(s) of the affected device, system or network that a problem has occurred and access and/or usage must be limited and/or halted until the problem is resolved
- Document ongoing analysis as appropriate on the Security Incident Response Form

Containment

- If *Cardholder Data* (CHD) is involved:
  - Do not access or alter compromised system(s) (e.g., do not log on to the compromised system(s) and change passwords; do not log in with administrative credentials). The compromised system(s) must be taken offline immediately and not be used to process payments or interface with payment processing systems.
  - Do not turn off, restart, or reboot the compromised system(s). Instead, isolate the compromised systems(s) from the rest of the network by unplugging the network cable(s) or through other means.
  - Preserve all evidence and logs (e.g. original evidence such as forensic image of systems and malware, security events, web logs, database logs, firewall logs, etc.).
  - Await further instruction from the ISSC or the V.P., Government Relations, Information Security and Privacy before proceeding with this process
- If *Cardholder Data* (CHD) is not involved:
  - Determine if it is necessary to disconnect the device from the Internet and/or the network
  - Determine if it is necessary to shut down the affected device, system, or network

    - Preserve all evidence and logs (e.g. original evidence such as forensic image of systems and malware, security events, web logs, database logs, firewall logs, etc.).
- Document and track all actions taken to contain the *security incident* on the Security Incident Response Form

Eradication

- Eradicate the problem that is affecting the device, system or network
- Determine whether disk drives should be cleaned/reformatted
- Ensure that previous device, system, and/or network file backups are not infected and take appropriate action
- Document and track all actions taken to eradicate all issues related to the security incident on the Security Incident Response Form

Restoration

- Decide whether the device, system and/or network needs to be restored from previous uninfected file backups
- Perform recovery procedures/processes as required
- Document and track all actions taken to restore workstation, network, system, etc. to its normal state on the Security Incident Response Form

Communication and Notification

- Communicate the appropriate information to the appropriate senior management personnel regarding the occurrence of the security incident (if a breach occurred)
- As warranted, notify the appropriate external entities (law enforcement, federal agency, state agency, Office of the Privacy Commissioner of Canada, payment card brands, payment card acquirers, customers, etc.) regarding the occurrence of the security incident (if a breach occurred involving credit card information or other personally identifiable information)
- If a user's workstation has to be reimaged due to a security incident, the user's manager will be notified and a copy of the Security Incident Response Form sent to the manager

Closure

- Ensure that the incident response process and the Cardholder Data Security Breach Response Process is updated with all lessons-learned and all appropriate industry developments regarding security incident or security breach response
- Ensure that all documentation, data, and/or information related to the security incident has been captured and is securely stored
- Ensure that all appropriate internal and external communication has been conducted as required

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at https://www.nist.gov/cyberframework/new-framework. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Policies, processes, and procedures around asset management generally follow the direction set by the Corporate Security Policy and are managed consistently with their relative importance to organizational objectives. We are working towards the implementation of a high-level risk strategy in upcoming years.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Policies, processes, and procedures generally follow the direction set by the Corporate Security Policy in these areas.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Policies, processes, and procedures generally follow the direction set by the Corporate Security Policy in these areas.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Policies, processes, and procedures around risk management generally follow the direction set by the Corporate Security Policy and are managed consistently with their relative importance to organizational objectives. We are working towards the implementation of a high-level risk strategy in upcoming years.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Policies, processes, and procedures around risk management generally follow the direction set by the Corporate Security Policy and are managed consistently with their relative importance to organizational objectives. We are working

Function	Category	Contractor Response
		towards the implementation of a high-level risk strategy in upcoming years.
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	The organization reviews and mitigates supply chain risks on a regular basis.
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Active Directory and Multi-factor authentication is used to access backend end system. Web user access is controlled using local authentication. Industry best practices are used for password strength.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	Security training and acknowledgement of our corporate information security policy is required for all staff and contractors annually and immediately upon hire.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	All connections are transmitted over secure channels using strong encryption (TLS 1.2). persistent data stored (at rest) is encrypted within our Microsoft Azure Cloud services. Systems and data are managed in a way that is consistent with our corporate information security policy.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Policies, processes, and procedures generally follow the direction set by the Corporate Security Policy in these areas. For instance, access is granted using a least-privilege model based on need. Where resources permit, access is granted based on defined roles and separation of duties.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Automated Backups are conducted regularly. Maintenance and repairs of the physical components are managed by Microsoft within the Azure Cloud.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Technical tools used are consistent with our policies, procedures, and agreements. For instance, tools such Web vulnerability scanners are deployed to identify potential risks and guide remediation efforts.

Function	Category	Contractor Response
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Azure PaaS services provides infrastructure Anomaly and Event management features via Microsoft Defender for App Services.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Azure PaaS services provides infrastructure Anomaly and Event management features via Microsoft Defender for App Services.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Azure PaaS services provides infrastructure Anomaly and Event management features via Microsoft Defender for App Services.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Incidents are managed in a way that is consistent with our corporate information security policy and incident response process.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Our incident response procedures call for this type of communications.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Our incident response procedures call for this type of activity.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Our incident response procedures call for this type of activity.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	We continually assess and enhance our processes to address the evolving threat environment as time and resources permit.
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Restoration of application and database assets are done using routinely taken backups in accordance with our incident response procedures.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Our incident response procedures call for this type of activity. Additionally, retrospectives are routinely conducted to discussion process improvements.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Our incident response procedures call for this type of activity. Internal and external communication is done on a case-by-case basis.