EXHIBIT

DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including

FRONTIER CENTRAL SCHOOL DISTRICT Bill of Rights for Data Security and Privacy
and
Supplemental Information about a Master Agreement between
FRONTIER CENTRAL SCHOOL DISTRICT and Bedford, Freeman & Worth Publishing Group, LLC

1. **Purpose**

(a) FRONTIER CENTRAL SCHOOL DISTRICT (hereinafter "District") and Bedford, Freeman & Worth Publishing Group, LLC (hereinafter "Vendor") are parties to a contract or other written agreement (which may be a purchase order) dated July 2022 (the "Master Agreement") pursuant to which Vendor will receive student data and/or teacher or principal data that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d") from the District for purposes of providing certain products or services (identified in Schedule 1 attached hereto (the "Product(s)") to the District pursuant to the Master Agreement.

(b) This Exhibit supplements the Master Agreement to which it is attached, to ensure that the Master Agreement conforms to the requirements of Section 2-d. This Exhibit consists of a Data Sharing and Confidentiality Agreement, a copy of the District's Bill of Rights for Data Security and Privacy signed by Vendor, and the Supplemental Information about the Master Agreement between FRONTIER CENTRAL SCHOOL DISTRICT and Bedford, Freeman & Worth Publishing Group, LLC that the District is required by Section 2-d to post on its website.

(c) In consideration of the mutual promises set forth in the Master Agreement, Vendor agrees that it will comply with all terms set forth in the Master Agreement and this Exhibit. To the extent that any terms contained in the Master Agreement or any terms contained in any other Exhibit(s) attached to and made a part of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect with respect to such conflict. In addition, in the event that Vendor has online or written Privacy Policies or Terms of Service (collectively, "TOS") that would otherwise be applicable to its customers or users of the products or services that are the subject of the Master Agreement between the District and Vendor, to the extent that any terms of the TOS, that are or may be in effect at any time during the term of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect with respect to such conflict.

2. **Definitions**

As used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor may receive from the District pursuant to the Master Agreement.

(b) “Teacher or Principal Data” means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Vendor may receive from the District pursuant to the Master Agreement.

(c) “Protected Data” means Student Data and/or Teacher or Principal Data, to the extent applicable to the Product(s) actually being provided to the District by Vendor pursuant to the Master Agreement. The term “Protected Data” does not include any information made publicly available by the District or any de-identified data or anonymized data.

(d) “NIST Cybersecurity Framework” means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the Master Agreement originates from the District and that this Protected Data belongs to and is owned by the District.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and the terms of this Data Sharing and Confidentiality Agreement.

(c) The District understands and agrees that the Vendor will process information in connection with the use of the Product(s) by District and its authorized users, including but not limited to, Protected Data pertaining to users of the Product. District hereby grants Vendor a license to use all such information: i) as reasonable required to provide the Product; and ii) to de-identify (as defined in FERPA) the Protected Data obtained hereunder and analyze it to improve Vendor’s educational products and services, including to create aggregated or statistical insights and baseline reports that are not identifiable to individuals or institutions for use in other Vendor educational products and services. The rights granted in this section 3(c) shall survive the expiration or termination of this agreement and supersedes any retention/deletion requirements herein.

4. **Data Security and Privacy Plan**

As more fully described herein, throughout the term of the Master Agreement, Vendor will have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from the District.

Vendor's Plan for protecting the District's Protected Data includes, but is not limited to, its agreement to comply with the terms of the District's Bill of Rights for Data Security and Privacy, a copy of which is set forth below and has been signed by the Vendor.

Additional components of Vendor's Data Security and Privacy Plan for protection of the District's Protected Data throughout the term of the Master Agreement are as follows:

(a) Vendor will implement all applicable state, federal, and local data security and privacy requirements including those contained within the Master Agreement and this Data Sharing and Confidentiality Agreement.

(b) Vendor will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the District under the Master Agreement.

(c) Vendor will comply with all obligations contained within the section set forth in this Exhibit below entitled "Supplemental Information about a Master Agreement between FRONTIER CENTRAL SCHOOL DISTRICT and Bedford, Freeman and Worth Publishing Group, LLC. Vendor's obligations described within this section include, but are not limited to:

(i) its obligation to require subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) to execute written agreements acknowledging that the data protection obligations imposed on Vendor by state and federal law and the Master Agreement shall apply to the subcontractor, and

(ii) its obligation to follow certain procedures for the deletion and/or destruction of Protected Data upon termination, expiration or assignment (to the extent authorized) of the Master Agreement.

(d) Vendor has provided or will provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees who will have access to Protected Data, prior to their receiving access and Vendor will ensure that its subcontractors or assigns are obligated to perform materially similar activities as those set forth in this section (d).

(e) Vendor will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches and unauthorized disclosures. Vendor will provide prompt notification to the District of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement.

5. **Notification of Breach and Unauthorized Release**

(a) Vendor will promptly notify the District of any breach or unauthorized release of Protected Data it has received from the District in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to the District by contacting Michael Sullivan directly by email at msullivan2@frontiercsd.org or by calling 716-926-1743

(c) To the extent legally permissible, Vendor will cooperate with the District and provide as much information as possible directly to Michael Sullivan or his/her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the District affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, the District, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor agrees not to provide this notification to the CPO directly unless requested by the District or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by the District, Vendor will promptly inform Michael Sullivan or his/her designee.

6. **Additional Statutory and Regulatory Obligations** [1]

Vendor acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received from the District, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the Master Agreement and the terms of this Data Sharing and Confidentiality Agreement:

(a) To limit internal access to Protected Data to only those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA); *i.e.*, they need access in order to assist Vendor in fulfilling one or more of its obligations to the District under the Master Agreement and this Data Sharing and Confidentiality Agreement.

(b) To not use Protected Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and the Master Agreement to which this Exhibit is attached.

(c) To not disclose any Protected Data to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations to the District and in compliance with state and federal law, regulations and the terms of the Master Agreement, unless:

[1] Nothing in Education Law Section 2-d or Part 121 specifically requires an educational agency to include within its contracts with third-party contractors this list of obligations that are imposed on third-party contractors by the statute and/or its implementing regulations. However, many school districts and other educational agencies have considered it a best practice to include these statutory and regulatory obligations within their third-party contracts.

(i) the parent or eligible student has provided prior written consent; or
(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to the District no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(d) To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.

(e) To use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5 and/or which aligns with the NIST Cybersecurity Framework.

(f) To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

(g) To comply with the data security and privacy terms set forth in this Data Sharing and Confidentiality Agreement, and Section 2-d and Part 121.

(h) To not sell Protected Data nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

(i) To notify the District, in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement, of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of applicable state or federal law, the District's Bill of Rights for Data Security and Privacy, or other binding obligations relating to data privacy and security contained in the Master Agreement and this Exhibit.

(j) To the extent legally permissible, to cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

(k) To pay for or promptly reimburse the District for the full cost of notification that the District is legally required to incur, in the event the District is required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor's breach of its obligations in this Data Sharing and Confidentiality Agreement.

Bill of Rights for Data Security and Privacy

FRONTIER CENTRAL SCHOOL DISTRICT

Section
Non-Instructional/Business Operations

Title
Information Security Breach and Notification

Code
5672

Status
Active

Adopted
April 23, 2013

Last Revised
February 11, 2020

Last Reviewed
February 11, 2020

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION

The District values the protection of private information of individuals in accordance with applicable law and regulations. Further, the District is required to notify affected individuals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy.

a) "Personal information: means any information concerning a person which, because of name, number, symbol, mark, or other identifier, can be used to identify that person.

b) "Private information" means either:

1. Personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted or encrypted with an encryption key that has also been accessed or acquired:

a) Social security number;
b) Driver's license number or non-driver identification card number;
c) Account number, credit or debit card number, in combination with any required security code, access code, password, or other information which would permit access to an individual's financial account;

d) Account number, credit or debit card number, if circumstances exist where the number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or
e) Biometric information, meaning data generated by electronic measurements of an individuals' unique physical characteristics, such as fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation which are used to authenticate or ascertain the individual's identity;

2. A username or email address in combination with a password or security question and answer that would permit access to an online account.

Private information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

c) "Breach of the security of the system" means unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the District. Good faith acquisition of personal information by an employee or agent of the District for the purposes of the District is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Determining if a Breach Has Occurred

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or person without valid authorization, the District may consider the following factors, among others:

a) Indications that the information is in the physical possession or control of an unauthorized person, such as a lost or stolen computer or other device containing information;

b) Indications that the information has been downloaded or copied;

c) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or

d) System failures.

Notification Requirements

a) For any computerized data owned or licensed by the School District that includes private information, the District shall disclose any breach of the security of the system following discovery or notification of the breach to any New York State resident whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure to affected individuals shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the integrity of the data system. The District will consult with the New York State Office of Information Technology Services to determine the scope of the breach and restoration measures. Within 90 days

of the notice of the breach, the New York State Office of Information Technology Services will deliver a report to the District on the scope of the breach and recommendations to restore and improve the security of the system.

b) Notice to affected persons under State Technology Law is not required if the exposure of of private information was an inadvertent disclosure by persons authorized to access private information, and the District reasonably determines the exposure will not likely result in the misuse of the information, or financial or emotional harm to the affected persons. This determination must be documented in writing and maintained for at least five years. If the incident affected over 500 New York State residents, the District will provide the written determination to the New York State Attorney General within ten days after the determination.

c) If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under certain laws and regulations, the District is not required to provide additional notice to those affected persons under State Technology Law. However, the District will still provide notice to the New York State Attorney General, the New York State Department of State, the New York State Office of Information Technology Services, and to consumer reporting agencies.

d) For any computerized data maintained by the District that includes private information which the District does not own, the District will notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.

The notification requirement may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. The required notification will be made after the law enforcement agency determines that the notification does not compromise the investigation.

If the District is required to provide notification of a breach, including breach of information that is not private information, to the United States Secretary of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act, it will provide notification to the New York State Attorney General within five business days of notifying the United State Secretary of Health and Human Services.

Methods of Notification

The required notice will be directly provided to the affected persons by one of the following methods:

a) Written notice;

b) Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and a log of each notification is kept by the District when notifying affected persons in electronic form. However, in no case will the District require a person to consent to accepting the notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

c) Telephone notification, provided that a log of each notification is kept by the District when notifying affected persons by phone; or

d) Substitute notice, if the District demonstrates to the New York State Attorney General that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or that the District does not have sufficient contact information. Substitute notice will consist of all of the following:

1. Email notice when the District has an email address for the subject persons;

2. Conspicuous posting of the notice on the District's website page, if the District maintains one; and

3. Notification to major statewide media.

Regardless of the method by which notice is provided, the notice will include:

a) Contact information for the notifying District;

b) The telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information; and

c) A description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have bee, accessed or acquired.

In the event that any New York State residents are to be notified, the District will notify the New York State Attorney General, New York State Department of State, and New York State Office of Information Technology Services as to the timing, content and distribution of the notices and approximate number of affected persons and provide a copy of the template of the notice sent to affected persons. This notice will be made without delaying notice to affected New York State residents.

In the event that more than 5,000 New York State residents are to be notified at one time, the District will also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. This notice will be made without delaying notice to affected New York State residents.

A list of consumer reporting agencies will be compiled by the New York State Attorney General and furnished upon request to any district required to make a notification in accordance with State Technology Law.

State Technology Law Sections 202 and 208

Adopted: 4/23/13
Revised: 11/17/15; 2/11/20

BY THE VENDOR:

Tonya Stoll

Name (Print)

Signature

VP of Operations

Title

6/2/2022

Date

Supplemental Information about a Master Agreement between

FRONTIER CENTRAL SCHOOL DISTRICT and Bedford, Freeman & Worth Publishing Group, LLC

FRONTIER CENTRAL SCHOOL DISTRICT has entered into a Master Agreement with Bedford, Freeman & Worth Publishing Group, LLC, which governs the availability to the District of the products identified in Schedule 1 attached to the Master Agreement (the "Product(s)")

Pursuant to the Master Agreement (which includes a Data Sharing and Confidentiality Agreement), the District may provide to Vendor, and Vendor will receive, personally identifiable information about students and/or teachers and principals that is protected by Section 2-d of the New York Education Law through the use of the Product(s) by the District and its authorized users ("Protected Data").

Exclusive Purposes for which Protected Data will be Used: The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the District with the Product(s) listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Master Agreement.

Oversight of Subcontractors: In the event that Vendor engages subcontractors or other authorized persons or entities to perform one or more of its obligations under the Master Agreement (including subcontracting hosting of the Protected Data to a hosting service provider), it will require those subcontractors or other authorized persons or entities to whom it will disclose the Protected Data to execute legally binding agreements acknowledging their obligation under Section 2-d of the New York Education Law to comply with all applicable data protection, privacy and security requirements required of Vendor under the Master Agreement and applicable state and federal law and regulations.

Duration of Agreement and Protected Data UponTermination or Expiration:

- The Master Agreement commences on _____ and expires on _____.
- Without undue delay following Vendor's receipt of a written request from District after the expiration of the Master Agreement without renewal, or termination of the Master Agreement prior to its expiration, Vendor will securely delete or otherwise destroy any and all personally identifiable information in the Protected Data remaining in the possession of Vendor or any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any personally identifiable information in the Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever except as otherwise set forth above. Without undue delay following Vendor's receipt of a written request from the District following such destruction, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed

Protected Data, as applicable, will provide the District with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by the District to Vendor, by contacting the District regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may request to challenge the accuracy of APPR data provided to Vendor by following the appeal process in the District's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data that Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States and the locations identified at the end of the document in this link: https://www.bfwpub.com/high-school/us/legal/privacy-notice#:~:text=When%20You%20are%20Required%20to,use%20our%20products%20and%20services. The measures that Vendor (and, if applicable, its subcontractors) will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework, and safeguards associated with industry standards and best practices including, but not limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (and, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology that complies with Section 2-d of the New York Education Law.

SCHEDULE 1

Vendor will use Protected Data to provide the following products and services (***please check all that apply***):

_____ **Achieve.** Achieve is a comprehensive set of interconnected teaching and assessment tools. It incorporates the most effective elements from Macmillan's market leading solutions - including Sapling, LaunchPad, iClicker and others - in a single, easy to use platform. Our resources were co-designed with instructors and students, using a foundation of learning research and rigorous testing.

_____ **Achieve Read and Practice** Achieve Read & Practice is the marriage of our LearningCurve adaptive quizzing and our mobile, accessible e-book, in one easy-to-use, affordable package. Learning Made Simple.

_____ **E-book** At roughly half the cost of the print text, e-books meet students where they already live—online.

_____ **FlipIt** FlipIt is a class preparation system for anybody looking for active learning or simply seeking a way to better prepare students for class.

_____ **iClicker.** iClicker's innovative classroom response system makes it easy to track attendance, increase participation, facilitate quizzes, measure performance, and get more out of your classroom.

_____ **iOLab** iOLab combines all the measurement devices and components needed for hundreds of physics labs in a single device, linking them to a software solution for gathering data and recording results. With iOLab, students are able to conduct Physics experiments from their own home with just the device and a computer.

_____ **Lab Simulations.** Hayden-McNeil Lab Simulations provide students with an authentic experience that moves laboratory learning beyond the classroom. With an editable lab manual, in-lab simulations and post-lab assessment, these interactive simulations allow Biology and Chemistry students to replicate the in-lab experience from the comfort of their own home with just an internet connection.

XX **LaunchPad** LaunchPad is a resource to help students achieve better results by providing a place where they can read, study, practice, complete homework, and more.

XX **Sapling & SaplingPlus** With Sapling Learning, every problem counts; student get wrong answer-specific feedback with nearly every problem so they learn from correct and incorrect answers and instructors get the support and analytics they need.

_____ **Writer's Help** With comprehensive content from authors you trust, Writer's Help 2.0 is an online writing resource that answers writers' questions and lets instructors track student achievement.

Vendor will also use Protected Data in accordance with the Agreement for customary business purposes, such as providing customer service and support, conducting user surveys, IT management (*e.g.,* user authentication, network security), creating de-identified data sets for analytics and other permitted purposes, for disaster recovery and business continuity, and for legal and regulatory compliance.