

EXHIBIT ____

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING

PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY AND SUPPLEMENTAL INFORMATION ABOUT THE Agreement

1. **Purpose**

(a) This Exhibit supplements the _____
(_____) agreement to which it is attached, to ensure that the AGREEMENT conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of the Burnt Hills-Ballston Lake Central School District's Parents Bill of Rights for Data Security and Privacy signed by xFanatical Inc _____ (hereby known as "vendor"), and the Supplemental Information about the Agreement that is required to be posted on the Burnt Hills-Ballston Lake Central School District's website.

(b) To the extent that any terms contained within the AGREEMENT, or any terms contained within any other Exhibits attached to and made a part of the AGREEMENT, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the AGREEMENT, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

Any capitalized term used within this Exhibit that is also found in the AGREEMENT will have the same definition as contained within the AGREEMENT.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, and the Family Educational Rights and Privacy Act (FERPA) 20 USC '1232-g, and the Individuals with Disabilities Education Act (IDEA) 20 USC ' 1400 et seq. from student records that vendor receives from a Participating Educational Agency pursuant to the AGREEMENT.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that vendor receives from a Participating Educational Agency pursuant to the AGREEMENT.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to vendor's Product.

(d) "Participating Educational Agency" means a school district within New York State that purchases instructional technology services and software through an AGREEMENT from a vendor or provider, and as a result is licensed to use vendor's Product pursuant to the terms of the AGREEMENT.

(e) "Breach" means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.

(f) "Eligible Student" means a student who is eighteen years or older.

(g) "Parent" means a parent, legal guardian or person in parental relation to a student.

(h) "Unauthorized Disclosure" or "Unauthorized Release" means any disclosure or release not permitted by federal or state statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the AGREEMENT may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(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, FERPA and IDEA) and the Burnt Hills-Ballston Lake Central School District's policy on data security and privacy. Vendor acknowledges that the Burnt Hills-Ballston Lake Central School District is obligated under Section 2-d to adopt a policy on data security and privacy, and the Burnt Hills-Ballston Lake Central School District can provide vendor with a copy of its policy if requested. Vendor and the Burnt Hills-Ballston Lake Central School District agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with the Burnt Hills-Ballston Lake Central School District's Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by vendor and is set forth below.

Additional elements of vendor's Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with the Burnt Hills-Ballston Lake Central School District's data security and privacy policy, vendor will: [attach the privacy policy plan regarding the Safe Doc product in this agreement.]

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the AGREEMENT, vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the AGREEMENT:

[Follow the NIST Cybersecurity Framework to implement strategic information protection measures.]

(c) Vendor will comply with all obligations set forth in the Burnt Hills-Ballston Lake Central School District's "Supplemental Information about the AGREEMENT" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows:

[Provide comprehensive training sessions to employees to manage protected data in xFanatical Safe Doc.

(e) Vendor [*check one*] ____ will ☒ will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the AGREEMENT. In the event that vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the AGREEMENT, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in the Burnt Hills-Ballston Lake Central School District's "Supplemental Information about the AGREEMENT," below, with comparable provisions related to confidentiality and data security, as well as employee and officer training.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identify breaches and unauthorized disclosures, and vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the AGREEMENT is terminated or expires, as more fully described in the Burnt Hills-Ballston Lake Central School District's "Supplemental Information about the AGREEMENT," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the AGREEMENT and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA), and consistent with the Individuals with Disabilities Education Act (IDEA). .

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist vendor in fulfilling one or more of its obligations under the AGREEMENT.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of vendor using the information to carry out vendor's obligations under the AGREEMENT, unless:

- (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 Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in the Burnt Hills-Ballston Lake Central School District's "Supplemental Information about the AGREEMENT," below.

(g) Provide notification to the Burnt Hills-Ballston Lake Central School District (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 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 state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse the Burnt Hills-Ballston Lake Central School District for the full cost of notification, in the event they are 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 or its subcontractors or assignees.

6. Notification of Breach and Unauthorized Release

(a) Vendor shall promptly notify the Burnt Hills-Ballston Lake Central School District of any breach or unauthorized release of Protected Data 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.

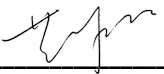
(b) Vendor will provide such notification to the Burnt Hills-Ballston Lake Central School District by contacting General Counsel directly by email at vanvranken@rvvlaw.com or by calling (518)399-2588 (office).

(c) Vendor will cooperate with the Burnt Hills-Ballston Lake Central School District and provide as much information as possible directly to the General Counsel or 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 personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies 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 Burnt Hills-Ballston Lake Central School 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 shall not provide this notification to the CPO directly. 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 Burnt Hills-Ballston Lake Central School District, vendor will promptly inform General Counsel or designees.

(e) Vendor will consult directly with General Counsel or designees prior to providing any further notice of the incident (written or otherwise) directly to the Burnt Hills-Ballston Lake Central School District.

BY Yetian Huang _____:

 _____ **Signature**

CEO _____ **Title**

2024-11-18 _____ **Date**

EXHIBIT ____ (CONTINUED)

PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

The Burnt Hills-Ballston Lake Central School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII)³ in educational records from unauthorized access or disclosure in accordance with State and Federal law. The Burnt Hills-Ballston Lake Central School District 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. Specifically, parents are assured:
 - that it is the district's policy to disclose personally identifiable information from student records, without consent, to other *school officials* within the district whom the district has determined to have *legitimate educational interests*. The notice will define 'school official' and 'legitimate educational interest.'

District policy P5500 provides the following definitions:

- *Legitimate Educational Interest*: a school official has a legitimate educational interest if they need to review a student's record in order to fulfill their professional responsibilities;
- *School Official*: a person who has a legitimate educational interest in a student record who is employed by the district as an administrator, supervisor, instructor or support staff member (including health or medical staff and law enforcement unit personnel); a member of the Board of Education; a person or company with whom the district has contracted to perform a special task (such as attorney, auditor, medical consultant or therapist); or a parent or student serving on an official committee, such as disciplinary or grievance committee, or assisting another school official performing their tasks.

- that, upon request, the district will disclose education records without consent to officials of another school district in which a student seeks to or intends to enroll or is actually enrolled.
 - that personally identifiable information will be released to third party authorized representatives for the purposes of educational program audit, evaluation, enforcement or compliance purposes.
 - that the district, at its discretion, releases directory information (see P5500) without prior consent, unless the parent/guardian or eligible student has exercised their right to prohibit release of the information without prior written consent. The district will not sell directory information.
 - that, upon request, the district will disclose a high school student's name, address and telephone number to military recruiters and institutions of higher learning unless the parent or secondary school student exercises their right to prohibit release of the information without prior written consent.
 - that the district will provide information as a supplement to the 'Parents' Bill of Rights' about third parties with which the district contracts that use or have access to personally identifiable student data.
 - that a student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by the district or any a third party contractor. The district will not sell student personally identifiable information. The district will not release it for marketing or commercial purposes, other than directory information released by the district in accordance with district policy;
- Parents¹ 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 AR-5500); Parents have the right to request that records be amended to ensure that they are not inaccurate, misleading, or otherwise in violation of the student's privacy rights;
 - State and federal laws³, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, and the Individuals with Disabilities Education Act protect the confidentiality of students' personally identifiable information. Specifically,
 - Parents have the right to consent to disclosure of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent; and
 - Parents have the right to file a complaint with the United States Department of Education alleging failure of the district to comply with FERPA and its regulations; and/or file a complaint regarding a possible data breach by a third party

contractor with the district and/or the New York State Education Department's Chief Privacy Officer for failure to comply with state law.

- 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 district's Data Protection Officer. 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 with 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 the District 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 district's Data Protection Officer (see www.bhbl.org).
- In the course of complying with its obligations under the law and providing educational services to District residents, the Burnt Hills-Ballston Lake Central School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are

defined by law and regulation. For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included in the contract and published on the District Web Page:

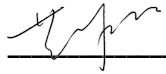
- The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
 - How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, 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);
 - The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
 - If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
 - Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
 - Address how the data will be protected using encryption while in motion and at rest.
- A parent or eligible student may challenge the accuracy of student data concerning that student or eligible student pursuant to the procedures provided for amendment of educational records under the Family Educational Rights and Privacy Act (FERPA).

¹ “Parent” means a parent, legal guardian, or person in parental relation to a student. These rights may not apply to parents of eligible students defined as a student eighteen years or older. “Eligible Student” means a student 18 years and older.

² “Personally identifiable information,” as applied to student data, means personally identifiable information as defined in section 99.3 of title thirty-four of the code of federal regulations implementing the family educational rights and privacy act, section twelve hundred thirty-two-g of title twenty of the United States code, and, as applied to teacher or principal data, means “personally identifying information” as such term is used in subdivision ten of section three thousand twelve-c of this chapter, and personal characteristics or information as such term is used under section 20 of the United States Code, section 1400 et seq., and implementing regulations at section 34 Code of Federal Regulations at 300.32. .

3 Information about other state and federal laws that protect student data such as the Children's Online Privacy Protection Act, the Protection of Pupil Rights Amendment, and NY's Personal Privacy Protection Law can be found at <http://www.nysed.gov/student-data-privacy/federal-laws-protect-student-data>.

BY Yetian Huang _____:



Signature

CEO

Title

2024-11-18

Date

EXHIBIT ____ (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE AGREEMENT BETWEEN Burnt Hills-Ballston Lake Central School District AND ____ (herby known as "vendor")

The Burnt Hills-Ballston Lake Central School District has entered into An Agreement ("AGREEMENT") with vendor ("xFanatical Inc _____"), which governs the availability to Participating Educational Agencies of the following Product(s): xFanatical Safe Doc

*[list scope of services from the Burnt Hills-Ballston Lake
Central School District to vendor]*

Pursuant to the AGREEMENT, Participating Educational Agencies may provide to vendor, and vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used:

To be completed by vendor:

The exclusive purpose for which vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly

authorized in the AGREEMENT. Protected Data received by vendor, or any of vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the AGREEMENT (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of vendor under the AGREEMENT and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: *[Describe steps the vendor will take]*

Duration of AGREEMENT and Protected Data Upon Expiration:

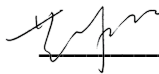
- The AGREEMENT commences on 2024-11-18 and expires on [date] by customer's xFanatical Safe Doc account closure date. Upon expiration of the AGREEMENT without renewal, or upon termination of the AGREEMENT prior to expiration, vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of vendor or its assignees or subcontractors. If requested by a Participating Educational Agency, vendor will assist that entity in exporting all Protected Data previously received for its own use, prior to deletion.
- At the Burnt Hills-Ballston Lake Central School District request, vendor will cooperate with the Burnt Hills-Ballston Lake Central School District as necessary in order to transition Protected Data to any successor vendor(s) prior to deletion.
- Vendor agrees that neither it nor its subcontractors, assignees, or other authorized agents will retain any copy, summary or extract of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, vendor and/or its subcontractors, assignees, or other authorized agents will provide 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 a Participating Educational Agency to vendor, by contacting the district's Information Officer regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to vendor by following the appeal process in the school district's applicable APPR Plan and applicable provisions of Section 8 of the New York Code of Rules and Regulations Part 30.

Data Storage and Security Protections: Any Protected Data 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. The measures that vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, 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 specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

BY Yetian Huang _____ :

 _____ **Signature**

CEO _____ **Title**

2024-11-18 _____ **Date**

xFanatical Safe Doc Privacy Policy

xFanatical Safe Doc is a chrome extension that manages inappropriate features in Google Workspace for Education to protect K-12 students from harmful content.

No Student Personal Data is collected

Safe Doc is compliant with COPPA, FERPA, PPRA, SOPIPA and SOPPA. We do NOT transmit, process, collect and sell any personally identifiable information (PII) of your students. All student data required by Safe Doc is encrypted and cached locally in students' school managed devices. By uninstalling Safe Doc from your students' managed devices, all cached data is deleted.

De-identified data (e.g. crash reporting) may be collected for Safe Doc troubleshooting and improvement. We ensure NO PII will be included in the de-identified data. We also do not attempt to re-identify de-identified data and do not disclose or transfer any of the de-identified data to third parties. As school officials, you may opt out such de-identified data collection using the Safe Doc configuration policy `OptOutAnonymousErrorReporting`.

For school accounts, we only store your students' domain name to verify your school license keys.

School Representative Data

If you're the school representative who applied for the trial or annual license, the information you provided is stored in our system for service purposes. We do not disclose, sell or rent your Personal Data to any unaffiliated third parties. Personal data collected from you may include but not limit to

- Your full name
- Your contact email
- Your school's student email domain(s)
- Your school's billing address, including an optional phone number
- Your school's purchase orders

If you use Safe Doc customer portal, you are subject to an additional data privacy term. We use Google reCaptcha to protect our software application from unauthorized accesses. Apart from the information provided you provide, consider visiting the Google reCaptcha privacy policies. Your data is protected by encryption-in-transit and encryption-at-rest.

To remove your Safe Doc account data permanently from our system, you need to request us (contact@xfanatical.com) in writing from the authorized email addresses in your Safe Doc account. We do not accept unauthorized requests.

To learn more, please visit xFanatical Privacy Policy at <https://xfanatical.com/privacy-policy>.