OREGON STUDENT DATA PRIVACY AGREEMENT
Version 1.0

BEAVERTON SCHOOL DISTRICT

and

TURNITIN, LLC

April 5, 2019

This Oregon Student Data Privacy Agreement ("DPA") is entered into by and between the Beaverton School District (hereinafter referred to as "LEA") and Turnitin, LLC (hereinafter referred to as "Provider") on April 5, 2019. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated _____ April 5, 2019 ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Federal Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state student privacy laws, including SB 187, Oregon Student Information Protection Act ("OSIPA"), Or. Rev. Stat. § 646.607 – 646.652; Or. Rev. Stat. § 326.565, et seq. (Student Records); and

WHEREAS, this Agreement complies Oregon laws and Federal Law.

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms", agree to allow other LEAs in Oregon the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, OSIPA and other applicable Oregon State laws, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA.

2. **Nature of Services Provided**. The Provider has agreed to provide the following digital educational services described below and as may be further outlined in Exhibit "A" hereto:

Insert Description

3. **Student Data to Be Provided**. In order to perform the Services described in the Service Agreement, LEA shall provide the categories of data described below or as indicated in the Schedule of Data, attached hereto as Exhibit "B":

Insert Description

4. **DPA Definitions**. The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over term used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data on the pupil's records, erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than 45 days from the date of the request) to the LEA's request for Student Data in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. Provider shall, at the request of the LEA, transfer Student Generated Content to a separate student account.

4. **Third Party Request**. Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services Agreement, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party unless legally prohibited. Provider shall share Student Data with law enforcement if required by law or court order. The Provider will not use, disclose, compile, transfer, sell the Student Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Student Data and/or any portion thereof.

5. **No Unauthorized Use**. Provider shall not use Student Data for any purpose other than as explicitly specified in the Service Agreement.

6. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With FERPA**. LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, OSIPA and all other Oregon privacy statutes quoted in this DPA.

2. **Annual Notification of Rights.** If the LEA has a policy of disclosing education records under 4 CFR § 99.31 (a) (1), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its Annual notification of rights, and determine whether Provider qualifies as a school official.

3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable State and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, OSIPA and all other Oregon privacy statutes identified in this DPA.

2. **Authorized Use**. The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above.

3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure**. De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data.

5. **Disposition of Data**. Upon written request, Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. The duty to dispose of Student Data shall not extend to data that has been de- identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Directive for Disposition of Data" FORM, (attached hereto as Exhibit "D"). Upon receipt of a written request from the LEA, the Provider will promptly provide the LEA with any specified portion of the Student Data within ten (10) business days of receipt of said request.

6. **Advertising Prohibition**. Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to Client; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to Client. This section does not prohibit Provider from generating legitimate personalized learning recommendations.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices within the educational technology industry, and to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

    a. **Passwords and Employee Access**. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding

said Student Data.

b. **Destruction of Data**. Upon written request, Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained

or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonably agree. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.

c. **Security Protocols**. Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.

d. **Security Technology**. Provider shall employ internet industry standard measures to protect data from unauthorized access while the data is in transit or at rest. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.

e. **Periodic Risk Assessment**. Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

f. **Backups.** Provider agrees to maintain backup copies, backed up at least daily, of Student Data in case of Provider's system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.

g. **Audits.** Upon reasonable written notice and request from the LEA, the LEA may reasonably audit the Provider to verify compliance with this DPA.

2. **Data Breach**. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident.

ARTICLE VI- GENERAL OFFER OF TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other LEA who signs the acceptance on said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b).

4. **Priority of Agreements**. This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific

mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives below:
The designated representative for the Provider for this DPA is:

Name: Bobby Wilson
Title: Chief Financial Officer
Contact Information:
2101 Webster St, Suite 1800

Oakland CA 94612. contracts@turnitin.com

The designated representative for the LEA for this DPA is:

Jim Newton, Manager of Application Development

6. **Entire Agreement**. This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties.

7. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE IN WHICH THIS DPA IS PERFORMED, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY IN WHICH THIS DPA IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority.** Provider represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof is stored, maintained or used in any way.

10. **Waiver**. No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this Oregon Student Data Privacy Agreement as of the last day noted below.

Turnitin, LLC

BY:  * Date: April 5, 2019

Printed Name: Chris Caren Title/Position:. CEO.
* Laura DiPiano for Chris Caren

Address for Notice Purposes: Turnitin, LLC.
Business Affairs
2101 Webster Street, Suite 1800
Oakland, CA 94612

Beaverton School District

BY: Ngoc Le Digitally signed by Ngoc Le Date: 2019.10.22 08:20:18 -07'00' Date: 10/22/2019

Printed Name: Ngoc Le Title/Position: Senior Purchasing Agent

Address for Notice Purposes:

16550 SW Merlo Road, Beaverton, OR 97003

EXHIBIT “A”

'Software-as-a-Service' providing plagiarism detection and educational feedback provision capabilities for LEAs. Student Data is stored at the direction of the LEA and depending on the LEA's preference, is compared against the and/or added to Contractor's database of submissions and internet resources. Storage of Student Data is usually indefinite at the request of the LEA so that it can be checked against in the future, but the LEA has the opportunity to not have its submissions stored at the end of the contract term.

When an LEA's Student Data is stored on the global database (as opposed to an 'institution only' database), and a text match is detected against a submission from a different LEA or educational institution, only the specific section of text that is matched against will be displayed to the 3rd party LEA/institution (but not the personal details of the author) which constitutes a partial disclosure of Student Data pursuant to Article III (3) herein which the LEA hereby consents to.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	x
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	x
Assessment	Standardized test scores	
	Observation data	x
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	

Category of Data	Elements	Check if used by your system
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	x
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	

Category of Data	Elements	Check if used by your system
	Low income status	
	Medical alerts /health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Category of Data	**Elements**	**Check if used by your system**
Student Contact Information	Address	
	Email	x
	Phone	
Student Identifiers	Local (School district) ID number	x
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	x
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading	

Category of Data	Elements	Check if used by your system
	program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	x
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data -Please	

Category of Data	Elements	Check if used by your system
	specify:	
Other	Please list each additional data	

Category of Data	Elements	Check if used by your system
	element used, stored or collected by your application	

EXHIBIT "C"

DEFINITIONS

ACPE (Association for Computer Professionals in Education): Refers to the membership organization serving educational IT professionals in the states of Oregon and Washington to promote general recognition of the role of IT professionals in educational institutions; improve network and computer services; integrate emerging technologies; encourage appropriate use of information technology for the improvement of education and support standards whereby common interchanges of electronic information can be accomplished efficiently and effectively.

Covered Information: Covered Information means materials that regard a student that are in any media or format and includes materials as identified by Oregon SB 187 (2015). The categories of Covered Information under Oregon law are found in Exhibit B. For purposes of this DPA, Covered Information is referred to as Student Data.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, and test protocols. For purposes of this DPA, Educational Records are referred to as Student Data.

De-Identifiable Information (DII): De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

Operator: The term "Operator" means the operator of an Internet Website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Service Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in applicable state statues.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or student-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

Provider: For purposes of the Service Agreement, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of student records. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

Student Records: Means both of the following: (1) Any information that directly relates to a student that is maintained by LEA and (2) any information acquired directly from the student through the use of instructional software or applications assigned to the student by a teacher or other LEA employee. For the purposes of this DPA, Student Records shall be the same as Educational Records, Student Personal Information and Covered Information.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School Official: For the purposes of this DPA and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1)

Performs an institutional service or function for which the agency or institution would otherwise use employees; and (2) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifiers, search activity, photos, voice recordings or geolocation information.
Student Data shall constitute Student Records for the purposes of this DPA, and for the purposes of Oregon and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

Student Personal Information: "Student Personal Information" means information collected through a school service that personally identifies an individual student or other information collected and maintained about an individual student that is linked to information that identifies an individual student. For purposes of this DPA, Student Personal Information is referred to as Student Data.

Subscribing LEA: An LEA that was not party to the original Services Agreement and who accepts the Provider's General Offer of Privacy Terms.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of student records. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

_____ Beaverton School District directs Turnitin, LLC ("Company") to dispose of data obtained by Company pursuant to the terms of the Service Agreement between LEA and Company. The terms of the Disposition are set forth below:

1. Extent of Disposition

____Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

Insert categories of data

_____Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

___Disposition shall be by destruction or deletion of data.

___Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

Insert Special Instructions

3. Timing of Disposition

Data shall be disposed of by the following date:

____As soon as commercially practicable

_____By

4. Signature

_____ _____
Authorized Representative of LEA Date

5. Verification of Disposition of Data

_____ _____
Authorized Representative of Company Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Beaverton School District and which is dated 4/5/2019 to any other LEA ("Subscribing LEA") who accepts this General Offer though its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by the Subscribing LEA to the Provider in Exhibit B to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; or (2) a material change in the services and products listed in the Originating Service Agreement. Provider shall notify either the ACPE or SDPC in the event it withdraws Exhibit E so that the withdrawal may be transmitted to the LEA.

Turnitin, LLC

BY: _____ Date: April 5, 2019

Printed Name: Chris Caren Title/Position: CEO

*Laura DiPiano for Chris Caren

2. Subscribing LEA _____ (Insert the Name of the Subscribing LEA)

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

BY: _____ Date: _____

Printed Name: _____ Title/Position _____

EXHIBIT “F” DATA SECURITY REQUIREMENTS

Insert additional data security requirements - None

Signature Certificate

Document Reference: 4YMWMDJND4V5L69KGDXYX3

RightSignature
Easy Online Document Signing

Laura DiPiano
Party ID: ZVDP64J2I2N7JSUMLL4T9T
IP Address: 23.118.109.55
VERIFIED EMAIL: ldipiano@turnitin.com

Electronic Signature:

Multi-Factor
Digital Fingerprint Checksum **81770f41fbe10130b6be447f3c64dab6215bcf6c**

Timestamp	Audit
2019-07-03 08:03:40 -0700	All parties have signed document. Signed copies sent to: Contracts, Laura DiPiano, and Angela Rhee.
2019-07-03 08:03:39 -0700	Document signed by Laura DiPiano (ldipiano@turnitin.com) with drawn signature. - 4.79.43.190
2019-07-03 06:28:46 -0700	Document viewed by Laura DiPiano (ldipiano@turnitin.com). - 23.118.109.55
2019-07-03 01:56:39 -0700	Document created by Angela Rhee (arhee@turnitin.com). - 193.240.89.26

This signature page provides a record of the online activity executing this contract.