

Standard Student Data Privacy Agreement

**IL-NDPA Standard
Version 1.0**

Naperville CUSD 203

and

Microsoft Education

This Student Data Privacy Agreement (“DPA”) is entered into on the date of full execution (the “Effective Date”) and is entered into by and between:

[Naperville CUSD 203], located at [203 W Hillside Rd
Naperville, IL 60540] (the “Local Education Agency” or “LEA”) and
[Microsoft Education], located at [One Microsoft Way
Redmond, WA 98052-7329] (the “Provider”).

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“COPPA”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
 - If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
 - If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit “H”. (Optional)**
 - If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “Services”).
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: Roger Brunelle Title: CIO

Address: 203 W Hillside Rd, Naperville, IL 60540

Phone: 630-420-6473 Email: rbrunelle@naperville203.org

The designated representative for the Provider for this DPA is:

Name: Beth Dann Title: General Manager West-US Education

Address: One Microsoft Way Redmond, WA 98052-7329

Phone: 425-890-3333 Email: Beth.Dann@microsoft.com

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA: Naperville CUSD 203

By:  Date: August 10, 2021

Printed Name: Roger Brunelle Title/Position: CIO

Provider: Microsoft Education

By:  Date: 8/2/21

Printed Name: Beth Dann Title/Position: General Manager

STANDARD CLAUSES

Version 1.0

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 including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, 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. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **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 terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

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 DPA 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 LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student 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.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests.** Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 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.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known 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 federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider’s employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student 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.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or

permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal

agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth set forth in Exhibit "F". Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to Exhibit "H". Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in Exhibit "F". Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
 - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as Exhibit "E"), be bound by the terms of Exhibit "E" 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. **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. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data 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, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit H, the SDPC Standard Clauses, and/or the Supplemental State Terms, Exhibit H will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute 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. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **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.

6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, 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 OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party 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.

9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"
DESCRIPTION OF SERVICES

Please see Addendum A for description of services.

Note: Information in this document assumes users are on M365 A5.

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.	<input type="checkbox"/>
	Other application technology meta data-Please specify:	<input type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input checked="" type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>
	Other assessment data-Please specify:	<input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input checked="" type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>
Communications	Online communications captured (emails, blog entries)	<input checked="" type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>
Demographics	Date of Birth	<input type="checkbox"/>
	Place of Birth	<input type="checkbox"/>
	Gender	<input type="checkbox"/>
	Ethnicity or race	<input type="checkbox"/>
	Language information (native, or primary language spoken by student)	<input type="checkbox"/>
	Other demographic information-Please specify:	<input type="checkbox"/>
Enrollment	Student school enrollment	<input type="checkbox"/>
	Student grade level	<input type="checkbox"/>
	Homeroom	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/>
	Year of graduation	<input type="checkbox"/>
	Other enrollment information-Please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Phone	<input type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input type="checkbox"/>
Schedule	Student scheduled courses	<input type="checkbox"/>
	Teacher names	<input type="checkbox"/>
Special Indicator	English language learner information	<input type="checkbox"/>
	Low income status	<input type="checkbox"/>
	Medical alerts/ health data	<input type="checkbox"/>
	Student disability information	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>
	Other indicator information-Please specify:	<input type="checkbox"/>
Student Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>
	Phone	<input type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input type="checkbox"/>
	State ID number	<input type="checkbox"/>
	Provider/App assigned student ID number	<input type="checkbox"/>
	Student app username	<input type="checkbox"/>
	Student app passwords	<input type="checkbox"/>
Student Name	First and/or Last	<input type="checkbox"/>
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input checked="" type="checkbox"/>
Student work	Student generated content; writing, pictures, etc.	<input checked="" type="checkbox"/>
	Other student work data -Please specify:	<input type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Student course grades/ performance scores	<input type="checkbox"/>
	Other transcript data - Please specify:	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other transportation data – Please specify:	<input type="checkbox"/>
Other	Please list each additional data element used, stored, or collected by your application: -	<input checked="" type="checkbox"/>
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	<input type="checkbox"/>

EXHIBIT "C" DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such 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, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

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 for K-12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. 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 in the services 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.

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; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

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, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or 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, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local 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.

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 service, and who has access to Student Data.

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

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

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 Education Records and/or Student Data, as that term is used in some state statutes. 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

Naperville CUSD 203

Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. 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:

[]

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:

[]

3. Schedule 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 [Naperville CUSD 203] ("Originating LEA") which is dated [_____], to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through 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 Subscribing LEA to the Provider 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; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed Exhibit "E" to Provider at the following email address:

_____.

Microsoft Education

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

2. 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 for the term of the DPA between the [Naperville CUSD 203] and the Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. ****

BY:

_____ Date: _____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone Number: _____

Email: _____

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider .

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
<input checked="" type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
<input checked="" type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input checked="" type="checkbox"/>	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input checked="" type="checkbox"/>	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
<input checked="" type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G" – Supplemental SDPC State Terms for Illinois
Version 1.0

This **Exhibit G**, Supplemental SDPC State Terms for Illinois ("Supplemental State Terms"), effective simultaneously with the attached Student Data Privacy Agreement ("DPA") by and between Naperville CUSD 203 (the "Local Education Agency" or "LEA") and Microsoft Education (the "Provider"), is incorporated in the attached DPA and amends the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

1. **Compliance with Illinois Privacy Laws.** In performing their respective obligations under the Agreement, the LEA and the Provider shall comply with all Illinois laws and regulations pertaining to student data privacy and confidentiality, including but not limited to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/.

2. **Definition of "Student Data."** In addition to the definition set forth in **Exhibit C**, Student Data includes any and all "covered information," as that term is defined in Section 5 of SOPPA (105 ILCS 85/5), and Student Data shall constitute "school student records" as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)).

3. **School Official Designation.** Pursuant to Article I, Paragraph 1 of the DPA Standard Clauses, and in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose.

4. **Limitations on Re-Disclosure.** The Provider shall not re-disclose Student Data to any Third Party or affiliate without the express written permission of the LEA or pursuant to court order, unless such disclosure is otherwise permitted under SOPPA, ISSRA, FERPA, and MHDDCA. In the event a Third Party, including law enforcement or a government entity, contacts the Provider with a request or subpoena for Student Data in the possession of the Provider, the Provider shall redirect the Third Party to seek the data directly from the LEA. In the event the Provider is compelled to produce Student Data to a Third Party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure.

5. **Notices.** Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid.

6. **Parent Right to Access and Challenge Student Data.** The LEA shall establish reasonable procedures pursuant to which a parent, as that term is defined in 105 ILCS 10/2(g), may inspect and/or copy Student Data and/or challenge the accuracy, relevance or propriety of Student Data, pursuant to Sections 5 and 7 of ISSRA (105 ILCS 10/5; 105 ILCS 10/7) and Section 33 of SOPPA (105 ILCS 85/33). The Provider shall respond to any request by the LEA for Student Data in the possession of the Provider, for

purposes of affording a parent an opportunity to inspect and/or copy the Student Data, no later than 10 business days from the date of the request. In the event that a parent contacts the Provider directly to inspect and/or copy Student Data, the Provider shall refer the parent to the LEA, which shall follow the necessary and proper procedures regarding the requested Student Data.

7. **Corrections to Factual Inaccuracies.** In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, the LEA shall notify the Provider of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the factual inaccuracy and shall provide written confirmation of the correction to the LEA.

8. **Security Standards.** The Provider shall implement and maintain commercially reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect Student Data from unauthorized access, destruction, use, modification, or disclosure, including but not limited to the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the Student Data (a "Security Breach"). For purposes of the DPA and this **Exhibit G**, "Security Breach" does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure.

9. **Security Breach Notification.** In addition to the information enumerated in Article V, Section 4(1) of the DPA Standard Clauses, any Security Breach notification provided by the Provider to the LEA shall include:

- a. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and
- b. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.

10. **Reimbursement of Expenses Associated with Security Breach.** In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, including but not limited to costs and expenses associated with:

- a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;
- b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;
- c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA as a result of the security breach; and

- d. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.

11. **Transfer or Deletion of Student Data.** The Provider shall review, on an annual basis, whether the Student Data it has received pursuant to the DPA continues to be needed for the purpose(s) of the DPA. If any of the Student Data is no longer needed for purposes of the DPA, the Provider must delete such unnecessary Student Data or transfer to the LEA such unnecessary Student Data. The Provider shall effectuate such transfer or deletion of Student Data and provide written confirmation of said transfer or deletion to the LEA within thirty (30) calendar days of the operator becoming aware that the Student Data is no longer needed for purposes of the DPA.

If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the request.

12. **Public Posting of DPA.** Pursuant to SOPPA, the LEA shall publish on its website a copy of the DPA between the Provider and the LEA, including this **Exhibit G.**

13. **Subcontractors.** By no later than (5) business days after the date of execution of the DPA, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom Student Data may be disclosed. This list shall, at a minimum, be updated and provided to the LEA by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1).

EXHIBIT "H"
Additional Terms or Modifications
Version _____

LEA and Provider agree to the following additional terms and modifications:

This is a free text field that the parties can use to add or modify terms in or to the DPA. If there are no additional or modified terms, this field should read "None."

618-1/4715859.1

See Attached Exhibit H



Microsoft 365, Office 365, Enterprise Mobility + Security, and Windows 10 Subscriptions for Education

Jump to section

[Microsoft 365 Apps](#)
[Social, Lync, and storage](#)
[Project and task management](#)
[Endpoint and app management](#)
[Insider risk management](#)

[Email, calendar, and scheduling](#)
[Classroom tools](#)
[Automation, app building, and chatbots](#)
[Integr. protection](#)
[Windows](#)

[Meetings, calling, and chat](#)
[Knowledge, insights, and content](#)
[Analytics](#)
[Identity and access management](#)
[Information protection](#)
[Information governance](#)

[eDiscovery and auditing](#)

Microsoft 365					Office 365			Enterprise Mobility + Security		Windows 10	
A1 (Device license)	A3	A5	A5 Security (add-on)	A5 Compliance (add-on)	A1	A3	A5	A3	A5	Education A3	Education A5

Microsoft 365 Apps

- Desktop client apps¹
- Office Mobile apps²
- Office for the web
- Install apps on up to 5 PCs/Mac + 5 tablets + 5 smartphones
- Microsoft Editor premium features
- Multilingual user interface for Office applications

¹Includes Word, Excel, PowerPoint, Outlook, Access (PC only), and Publisher (PC only)

²Includes Word, Excel, PowerPoint, Outlook, and OneNote mobile Apps

Mobile apps only

Email, calendar, and scheduling

- Exchange
- Mailbox size
- Calendar
- Outlook desktop client
- Email archiving
- Public folder mailboxes
- Resource mailboxes
- Inactive mailboxes
- Microsoft Shifts
- Microsoft Bookings

Meetings, calling, and chat

- Microsoft Teams
- Live events
- Phone System
- Audio Conferencing¹
- Skype for Business Online

¹Check country and region availability at <https://aka.ms/teamsfeatures> and confirm availability for work, conferencing, and calling data

Microsoft 365					Office 365			Enterprise Mobility + Security		Windows 10	
A1 (Device licenses)	A3	A5	A5 Security (add-on)	A5 Compliance (add-on)	A1	A3	A5	A3	A5	Educational A3	Education A5

Social, intranet, and storage

- SharePoint
- Additional storage per license¹
- OneDrive personal storage
- Yammer Academic

¹In addition to 1TB storage provided per organization

²Microsoft will provide an initial 5 TB of OneDrive storage per user. Customers who want additional OneDrive storage can request it as needed by contacting Microsoft support. Subscriptions for fewer than five users receive 1 TB OneDrive storage per user.

Classroom tools

- Classroom experience in Microsoft Teams
- Microsoft Whiteboard
- OneNote Class Notebook
- Minecraft Education Edition with Code Builder
- Take a Test app
- Set up School PCs app

Knowledge, insights, and content

- Microsoft Graph API
- Microsoft Search
- Microsoft Stream
- Microsoft Forms
- Microsoft Lists
- Delve

Project and task management

- Microsoft Planner
- Microsoft To-Do
- Briefing Email

Automation, app building, and chatbots

- Power Apps for Microsoft 365¹
- Power Automate for Microsoft 365¹
- Power Virtual Agent for Teams¹
- Dataverse for Teams¹

¹Refer to the Licensing FAQs and Licensing Guide at <https://docs.microsoft.com/power-platform/admin/powerapps-faq> for details including functionality limits

²Cloud flows only; no desktop flows

³Desktop flows only; no cloud flows

	Microsoft 365					Office 365			Enterprise Mobility + Security		Windows 10	
	A1 (Device license)	A3	A5	A5 Security Addition	A5 Compliance Addition	A1	A3	A5	A3	A5	Education A3	Education A5

Analytics

- Compliance Management
- MyAnalytics
- Education Analytics
- Productivity Score
- Secure Score
- Power BI Pro

Endpoint and app management

- Microsoft Intune for Education
- Mobile Device Management
- Microsoft Endpoint Manager
- Windows AutoPilot
- Mobile application management
- Windows Hello for business
- Group Policy support
- Shared computer activation for M365 Apps
- Cortana management
- Endpoint Analytics

Threat protection

- Microsoft Defender Antimalware
- Microsoft Defender Firewall
- Microsoft Defender Exploit Guard
- Microsoft Defender Credential Guard
- BitLocker and BitLocker To Go
- Windows Information Protection
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Application Guard for Office 365
- Safe Documents

AI (Device license)	Microsoft 365				Office 365			Enterprise Mobility + Security		Windows 10	
	A3	A5	A5 Security (all on)	A5 Compliance (all on)	A1	A3	A5	A3	A5	Education A3	Education A5

Identity and access management

	Plan 1	Plan 2	Plan 2	Plan 1	Plan 2	Plan 1	Plan 2
Azure Active Directory Premium							
User Provisioning	•	•	•	•	•	•	•
Self Service Password Reset	•	•	•	•	•	•	•
Advanced Security Reports	•	•	•	•	•	•	•
Multi Factor Authentication	•	•	•	•	•	•	•
Conditional Access	•	•	•	•	•	•	•
Cloud App Security Discovery	•	•	•	•	•	•	•
Office 365 Cloud App Security	•	•	•	•	•	•	•
Microsoft Cloud App Security	•	•	•	•	•	•	•
Risk Based Conditional Access / Identity Protection							
Privileged Identity Management	•	•	•	•	•	•	•
Access Reviews	•	•	•	•	•	•	•
Entitlement Management	•	•	•	•	•	•	•
Microsoft 365 Groups	•	•	•	•	•	•	•
On-premises Active Directory sync for SSO	•	•	•	•	•	•	•
DirectAccess supported	•	•	•	•	•	•	•
Windows Hello for Business	•	•	•	•	•	•	•
Microsoft Advanced Threat Analytics	•	•	•	•	•	•	•
Windows Store Access Management	•	•	•	•	•	•	•

Information protection

	Plan 1	Plan 2	Plan 2	Plan 1	Plan 2	Plan 1	Plan 2
Azure Information Protection							
Manual sensitivity labels	•	•	•	•	•	•	•
Automatic sensitivity labels	•	•	•	•	•	•	•
Machine Learning-based sensitivity labels							
Office 365 Data Loss Prevention (DLP) for emails and files	•	•	•	•	•	•	•
Communication DLP (Teams chat)	•	•	•	•	•	•	•
Endpoint DLP	•	•	•	•	•	•	•
Basic Office Message Encryption	•	•	•	•	•	•	•
Advanced Office Message Encryption	•	•	•	•	•	•	•
Customer Key for Office 365	•	•	•	•	•	•	•



	Microsoft 365				Office 365			Enterprise Mobility + Security		Windows 10		
	A1 (Device license)	A3	A5	A5 Security Add-on	A5 Compliance Add-on	A1	A3	A5	A3	A5	Education A3	Education A5
Information governance												
Manual retention labels												
Basic org-wide or location-wide retention policies												
Rules-based automatic retention policies												
Machine Learning-based retention												
Teams retention policies												
Records Management												
eDiscovery and auditing												
Content Search												
Core eDiscovery (including Hold and Export)												
Litigation Hold												
Advanced eDiscovery												
Basic Audit												
Advanced Audit												
Insider risk management												
Insider Risk Management												
Communication Compliance												
Information Barriers												
Customer Lockbox												
Privileged Access Management												
Windows												
Windows 10 Edition												
Windows Virtual Desktop (WVD)												
Universal Print												

©2021 Microsoft Corporation. All rights reserved. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. This document does not provide you with any legal rights to any Microsoft product. Publish date: March 1, 2021

Exhibit H
Additional Terms or Modifications

LEA and Provider agree to the following additional terms and modifications:

STANDARD CLAUSES

Version 1.0

Article II, section 2, Parent Access.

Parties agree to delete this section as it is not applicable. The LEA has access to the data at all times and can provide.

Article II, section 4, Law Enforcement Requests.

Parties agree to delete this provision replace with following industry standard provision from Microsoft's Data Processing Addendum ("DPA") (which is incorporated by reference in the Online Services Terms ("OST") and which is also incorporated by reference in any Microsoft agreement for Online Services):

Nature of Data Processing; Ownership. *Microsoft will use and otherwise process Student Data only (a) to provide Online Services in accordance with the LEA's documented instructions, and (b) for Microsoft's legitimate business operations, each as detailed and limited below. As between the parties, the LEA retains all right, title and interest in and to Student Data. Microsoft acquires no rights in Student Data, other than the rights the LEA grants to Microsoft in this section. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to the LEA.*

Disclosure of Processed Data. *Microsoft will not disclose Processed Data except: (1) as the LEA directs; (2) as described in this DPA; or (3) as required by law. For purposes of this section, "Processed Data" means: (a) Customer Data; (b) Personal Data; and (c) any other data processed by Microsoft in connection with the Online Service that is the LEA's confidential information under the volume license agreement. All processing of Processed Data is subject to Microsoft's obligation of confidentiality under the volume license agreement.*

Microsoft will not disclose Processed Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Processed Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from the LEA. If compelled to disclose Processed Data to law enforcement, Microsoft will promptly notify the LEA and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third-party request for Processed Data, Microsoft will promptly notify the LEA unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from the LEA.

Microsoft will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Processed Data; (b) platform F keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, Microsoft may provide the LEA's basic contact information to the third party.

Article V, section 2, Audits.

Parties agree to delete this provision and replace with the following:

Microsoft will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data and Personal Data, as follows:

Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually.

Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.

Each audit will be performed by qualified, independent, third party security auditors at Microsoft's selection and expense.

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which Microsoft will make available at <https://servicetrust.microsoft.com/> or another location identified by Microsoft. The Microsoft Audit Report will be Microsoft's Confidential Information and will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor. If Customer requests, Microsoft will provide Customer with each Microsoft Audit Report. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Microsoft and the auditor.

To the extent Customer's audit requirements under the Standard Contractual Clauses or Data Protection Requirements cannot reasonably be satisfied through audit reports, documentation or compliance information Microsoft makes generally available to its customers, Microsoft will promptly respond to Customer's additional audit instructions. Before the commencement of an audit, Customer and Microsoft will mutually agree upon the scope, timing, duration, control and evidence requirements, and fees for the audit, provided that this requirement to agree will not permit Microsoft to unreasonably delay performance of the audit. To the extent needed to perform the audit, Microsoft will make the processing systems, facilities and supporting documentation relevant to the processing of Customer Data and Personal Data by Microsoft, its Affiliates, and its Subprocessors available. Such an audit will be conducted by an independent, accredited third-party audit firm, during regular business hours, with reasonable advance notice to Microsoft, and subject to reasonable confidentiality procedures. Neither Customer nor the auditor shall have access to any

data from Microsoft's other customers or to Microsoft systems or facilities not involved in the Online Services. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Microsoft expends for any such audit, in addition to the rates for services performed by Microsoft. If the audit report generated as a result of Customer's audit includes any finding of material non-compliance, Customer shall share such audit report with Microsoft and Microsoft shall promptly cure any material non-compliance.

If the Standard Contractual Clauses apply, then this section is in addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the Standard Contractual Clauses. Nothing in this section of the DPA varies or modifies the Standard Contractual Clauses or the GDPR Terms or affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses or Data Protection Requirements. Microsoft Corporation is an intended third-party beneficiary of this section.

Article V, section 3, Data Security.

Parties agree that the following further documentation on Microsoft's security commitments will apply and are incorporated into the contract via the Online Services Privacy & Security Terms, inclusive of the Data Protection Addendum, found at : Commercial Licensing Terms (microsoft.com).

Article V, section 4, Data Breach.

Parties agree to delete this provision and replace with the following industry standard provision from Microsoft's Data Processing Addendum ("DPA") (which is incorporated by reference in the Online Services Privacy and Security Terms:

***Security Incident Notification.** If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Student Data while processed by Microsoft (each a "Security Incident"), Microsoft will promptly and without undue delay (1) notify the LEA of the Security Incident; (2) investigate the Security Incident and provide the LEA with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.*

Notification(s) of Security Incidents will be delivered to one or more of the LEA's administrators by any means Microsoft selects, including via email. It is the LEA's sole responsibility to ensure the LEA's administrators maintain accurate contact information on each applicable Online Services portal. The LEA is solely responsible for complying with its obligations under incident notification laws applicable to the LEA and fulfilling any third-party notification obligations related to any Security Incident.

Microsoft shall make reasonable efforts to assist the LEA in fulfilling the LEA's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

Microsoft's notification of or response to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

The LEA must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

Exhibit F, Supplemental Terms to Data Security Requirements

Parties agree that the following further documentation on Microsoft's security commitments are hereby added to Exhibit F:

Many organizations in regulated industries are subject to extensive compliance requirements. To perform their own risk assessments, customers often need in-depth information about how Microsoft 365 maintains the security and privacy of their data. Microsoft is committed to the security and privacy of customer data in its cloud services and to earning customer trust by providing a transparent view of its operations, and easy access to independent compliance reports and assessments.

Service Assurance provides transparency of operations and information about how Microsoft maintains the security, privacy, and compliance of customer data in Microsoft 365. It includes third-party audit reports along with a library of white papers, FAQs, and other materials on Microsoft 365 topics such as data encryption, data resiliency, security incident management and more. Customers can use this information to perform their own regulatory risk assessments. Compliance officers can assign the "Service Assurance User" role to give users access to Service Assurance. The tenant administrator can also provide external users, such as independent auditors, with access to information in the Service Assurance dashboard through the Microsoft Cloud Service Trust Portal (STP).

Trust Center MSComplianceGuideV3 (microsoft.com)

- CIS Top 20 - Best practices for securely using Microsoft 365—the CIS Microsoft 365 Foundations Benchmark now available | Microsoft Security Blog
- ISO-27001 - ISO/IEC 27001:2013 Information Security Management Standards - Microsoft Compliance | Microsoft Docs
- CMMC L1-5 - CMMC Level 3 blueprint sample - Azure Blueprints | Microsoft Docs
- NIST 800-53 - National Institute of Standards and Technology (NIST) SP 800-53 - Azure Compliance | Microsoft Docs
- NIST 800-171 - NIST SP 800-171 - Microsoft Compliance | Microsoft Docs
- NIST CSF - NIST SP 800-171 - Microsoft Compliance | Microsoft Docs
- DFARS - Defense Federal Acquisition Regulation Supplement (DFARS) - Microsoft Compliance | Microsoft Docs

Exhibit “G” – Supplemental SDPC State Terms for Illinois

7. Corrections to Factual Inaccuracies.

Parties agree to delete this provision as it is inapplicable. Microsoft does not have the ability to correct data, only the LEA does.

9. Security Breach Notification.

Parties agree to delete this provision and replace with the following industry standard provision from Microsoft’s Data Processing Addendum (“DPA”) (which is incorporated by reference in the Online Services Privacy and Security Terms):

***9. Security Incident Notification.** If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Student Data while processed by Microsoft (each a “Security Incident”), Microsoft will promptly and without undue delay (1) notify the LEA of the Security Incident; (2) investigate the Security Incident and provide the LEA with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.*

Notification(s) of Security Incidents will be delivered to one or more of the LEA’s administrators by any means Microsoft selects, including via email. It is the LEA’s sole responsibility to ensure the LEA’s administrators maintain accurate contact information on each applicable Online Services portal. The LEA is solely responsible for complying with its obligations under incident notification laws applicable to the LEA and fulfilling any third-party notification obligations related to any Security Incident.

Microsoft shall make reasonable efforts to assist the LEA in fulfilling the LEA’s obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

Microsoft’s notification of or response to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

The LEA must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

10. Reimbursement of Expenses Associated with Security Breach.

Parties agree to delete this provision.

11. Transfer or Deletion of Student Data.

Parties agree to delete this provision as the LEA has the responsibility to delete its own data.

13. Subcontractors.

Parties agree to delete this provision and replace with the following industry standard provision:

***Subcontractors.** Microsoft may hire third parties to provide certain limited or ancillary services on its behalf. The LEA consents to the engagement of these third parties and Microsoft Affiliates as Subcontractors. The above authorizations will constitute the LEA's prior written consent to the subcontracting by Microsoft of the processing of Student Data.*


Microsoft is responsible for its Subcontractors' compliance with Microsoft's obligations under this Agreement. Microsoft makes available information about Subcontractors on a Microsoft website. When engaging any Subcontractor, Microsoft will ensure via a written contract that the Subcontractor may access and use Student Data only to deliver the services Microsoft has retained them to provide and is prohibited from using Student Data for any other purpose. Microsoft will ensure that Subcontractors are bound by written agreements that require them to provide at least the level of data protection required of Microsoft by this Agreement. Microsoft agrees to oversee the Subcontractors to ensure that these contractual obligations are met.

From time to time, Microsoft may engage new Subcontractors. Microsoft will give the LEA notice (by updating the website and providing the LEA with a mechanism to obtain notice of that update) of any new Subcontractor at least 6 months in advance of providing that Subcontractor with access to Student Data. Additionally, Microsoft will give the LEA notice (by updating the website and providing the LEA with a mechanism to obtain notice of that update) of any new Subcontractor at least 14 days in advance of providing that Subcontractor with access to data other than that which is contained in Student Data.

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

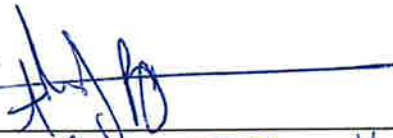
1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and [Naperville CUSD 203] ("Originating LEA") which is dated [], to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through 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 Subscribing LEA to the Provider 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; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed Exhibit "E" to Provider at the following email address:

Microsoft Education
BY:  Date: 9/13/21
Printed Name: Beth Dann Title/Position: General Manager
US Education

2. 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 for the term of the DPA between the [Naperville CUSD 203] and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

BY:  Date: 9/13/21
Printed Name: Andrew J. Barrett Title/Position: Assistant Superintendent
SCHOOL DISTRICT NAME: Geneva CUSD 304
DESIGNATED REPRESENTATIVE OF LEA:
Name: Michael Wilkes
Title: Director, Technology
Address: 227 North Fourth Street, Geneva, IL 60134
Telephone Number: 630-463-3070
Email: it@Geneva304.org

