Exhibit A

Parents Bill of Rights Relating to Student Data

The District, in compliance with Education Law 2-d, provides the following:

DEFINITIONS:
As used in this policy, the following terms are defined:

Student Data means personal identifiable information from the student records of a District student.

Teacher or Principal Data means personally identifiable information from District records relating to the annual professional performance reviews of classroom teachers or Principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

Third-Party Contractor means any person or entity, other than a District, that receives student data or teacher or Principal data from the District pursuant to a contract or other written agreement for purposes of providing services to the District, including, but not limited to, data management or storage services, conducting studies for or on behalf of the District, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student or teacher or Principal data from a school district to carry out its responsibilities pursuant to Education Law §211-e and is not a District, and a not-for-profit corporation or other nonprofit organization other than a District.

1. Neither student data, nor teacher or Principal data will not be sold or released for any commercial purpose;

2. Parents have the right to inspect and review the complete contents of their child's education record. Procedures for reviewing student records can be found in the Board Policy entitled: **#26 Policies and Procedures and Family Educational Rights and Privacy Act (FERPA) Notice for Directory Information** – *Section 1 – Legally Mandated Policies*;

3. Security protocols regarding confidentiality of personally identifiable information are currently in place and the safeguards necessary to protect the confidentiality of student data are maintained at industry standards and best practices. The safeguards include, but are not limited to encryption, firewalls, and password protection. As required by Education Law §2-d(5), the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF) is adopted as the standard for data security and privacy;

4. New York State maintains a complete list of all student data collected by the State and the data is available for public review at http://www.p12.nysed.gov/irs/sirs/NYSEDDataElements2018.xlsx or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234;

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to Records Access Officer, Joseph Gugino, Oxford Academy and Central School District, PO Box 192, Oxford, NY 13830;

6. The District will promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect personally identifiable information;

   - Following its investigation of a submitted complaint, the District shall provide the parent or eligible student with its findings within a reasonable period but no more than 60 calendar days from receipt of the complaint;

   - Where the District requires additional time, or where the response may compromise security or impede a law enforcement investigation, the District hall provide the parent or eligible student with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint;

   - The District will require complaints to be submitted in writing;

   - The District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1;

7. This policy will be regularly updated with supplemental information for each contract the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or Principal data. The supplemental information must be developed by the District and include the following information:

- The exclusive purposes for which the student data or teacher or Principal data will be used by the third-party contractor, as defined in the contract;

- How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or Principal data, if any, will abide by all applicable data protection and security requirements, including, but not limited to, those outlined in applicable State and federal laws and regulations (e.g., FERPA; Education Law §2-d);

- The duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or Principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the District and whether, when and how the data will be destroyed);

- If an how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or Principal data that is collected;

- Where the student data or teacher or Principal data will be stored, it will be described in such a manner as to protect data security and the security protections taken to ensure that such data will be protected and data security and privacy risks mitigated; and how the data will be protected using encryption while in motion and at rest will be addressed.

8. This policy shall be published on the District's website. This policy shall also be included with every contract the District enters with a third party contractor where the third party contractor receives student data or teacher or Principal data.

Agreement and Signature

By signing below, you agree to the Terms and Conditions in this Rider:

Company Name Microsoft Product Name Flipgrid

Printed Name Dr. Charles Miller Signature CDM Date 8/31/2020

Adopted 5/9/16

Amended 6/1/20

9/3/20

Oxford Academy, Date

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between __Oxford Academy & CSD_____ ("DISTRICT") and **Microsoft Corporation** ("**VENDOR**") to the contrary, **VENDOR** agrees as follows as to Flipgrid software and services:

VENDOR will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as **VENDOR** uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. **VENDOR** shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. **VENDOR** shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party.

"**Protected Data**" includes any information that is linked or reasonably linkable to a student including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of the DISTRICT and/or its Participants as that term is defined in 34 CFR §99.3, which implements the Family Educational Rights and Privacy Act ("FERPA"),
>
> -AND-
>
> Personally identifiable information from the records of the DISTRICT and/or its Participants relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law 3012-c.

VENDOR and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, **VENDOR** agrees to comply with the DISTRICT policy(ies) on data security and privacy provided such policies are attached to this Agreement. **VENDOR** shall promptly reimburse DISTRICT and/or its Participants for the full cost of notifying a parent, eligible student,

teacher, or principal of an unauthorized release of Protected Data by **VENDOR** its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, **VENDOR** shall return all of DISTRICT and/or its Participants' data, including any and all Protected Data, in its possession by secure transmission or delete all Protected Data as directed by DISTRICT. Either party may terminate this Agreement with 30 days' notice to the other party.

Data Security and Privacy Plan

VENDOR and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of DISTRICT and/or its Participant's Protected Data, pursuant to this agreement and for the specific purpose of providing the FlipGrid software and services to representatives of DISTRICT and students, including purposes compatible with providing those sevices, and shall maintain a Data Security and Privacy Plan that includes the following elements:

1. A provision incorporating the requirements of New York Parents' Bill of Rights for data security and privacy, to the extent that any of the provisions in the Bill of Rights applies to **VENDOR**'s possession and use of Protected Data pursuant to this Agreement.

2. An outline of how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the **VENDOR**'s policy on data security and privacy.

3. An outline of the measures taken by **VENDOR** to secure Protected Data and to limit access to such data to authorized staff.

4. An outline of how **VENDOR** will use "best practices" and industry standards with respect to data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored data to authorized staff.

5. An outline of how **VENDOR** will ensure that any subcontractors, persons or entities with which **VENDOR** will share Protected Data, if any, will abide by the requirements of **VENDOR**'s policy on data security and privacy, and the contractual obligations with respect to Protected Data set forth herein.

DATA PRIVACY AND SECURITY PLAN

1. Attached hereto as Exhibit "A" is a copy of the New York Parents' Bill of Rights signed by **VENDOR**.