Exhibit "G"
Supplemental Information

District and Code.org have entered into a Student Data Protection Addendum ("DPA"). The DPA supplements the Service Agreement and together with the Service Agreement, is collectively referred to as the "Agreement". The Service Agreement is defined as the Code.org Terms of Service located at https://code.org/tos (the "Service Agreement"). All terms not defined below or in the DPA shall have the meaning set forth in New York State Education Law §2-d ("Education Law §2-d").
required by Education Law §2-d(3)(c) and Section 121.3 of the implementing Regulations, the following is the "Supplemental Information" for the Agreement with the Contractor Code.org:

A. Use of Student Data: Student Data and/or Teacher or Principal Data which the Contractor comes into possession as part of its Agreement with the District shall be used for the following exclusive purpose(s):

Pursuant to and as fully described in the Service Agreement, Provider has agreed to provide the digital educational services set forth below and any other products and services that Provider may provide now or in the future (the "Services").

Services:

Code.org is a nonprofit dedicated to expanding participation in computer science by making it available in more schools, and increasing participation by women and underrepresented students of color.

As part of its mission to expand access to computer science Code.org provides the following services and resources:

- An online curriculum for teaching computer science, and an online learning platform for students to learn coding and computer science and to display and share their work
- Professional learning program for teachers to prepare to teach computer science
- Resources to support schools, districts, teachers, administrators, students, volunteers, parents, and advocates who want to expand the availability of computer science education, including recommendations of third party curriculum and course providers, links to educational resources, etc.
- Information about the state of computer science education in K-12 schools in America and globally
- Advocacy in support of Computer Science education in the K-16 education system
- The coordination and leadership of the global Hour of Code campaign for celebrating participation in computer science

B. Service Providers: The Contractor will ensure that any and all subcontractors, or other authorized persons or entities that the Contractor may disclose the Student Data and/or Principal or Teacher Data with, if any, ("Service Providers") will abide by the applicable data protection and security terms of the DPA and in Education Law §2-d and Part 121 of the Regulations. Contractor will do so by entering into written agreements with such Service Providers, whereby the Service Providers agree to protect Student Data and/or Principal or Teacher Data (if applicable) in a manner no less stringent than the terms of the DPA. The list of Provider's current Service Providers can be accessed through the Provider's Privacy Policy (which may be updated from time to time).

C. Term and Termination:

- **Term:** The duration of this Agreement coincides with the duration of the parties' underlying Service Agreement, which is currently set to expire on**:** The Service Agreement expires upon termination by either party as set forth in the Service Agreement or upon a material breach by either Party of the terms of the DPA.

- **Data Deletion upon Termination:** When the Agreement between the District and the Contractor expires or terminates, the Contractor shall: At District's request, dispose of or delete all Personally Identifiable Information contained in Student Data within a reasonable time period following a written request. If no written request is received, Contractor shall dispose of or delete all Personally Identifiable Information contained in Student Data at the earliest of (a) when it is no longer needed for the purpose for which it was obtained or (b) as required by applicable law. Nothing in the DPA authorizes Contractor to maintain Personally Identifiable Information contained in Student Data obtained under the Agreement beyond the time period reasonably needed to complete the disposition, unless a student, parent or legal guardian of a student chooses to establish and maintain a separate Personal Login with Contractor to retain Student Generated Content. Disposition shall include (1) the shredding of any hard copies of any Personally Identifiable Information contained in Student Data; (2) erasing any Personally Identifiable Information contained in Student Data; or (3) otherwise modifying the Personally Identifiable Information contained in Student Data to make it unreadable or indecipherable or De-Identified or maintained to use with a Personal Login, pursuant to the other terms of the DPA. Contractor shall provide written notification to District when the Personally Identifiable Information contained in Student Data has been disposed pursuant to the District's request for deletion. The duty to dispose of Student Data shall not extend to data that has been De-Identified.

D. **Parent Access and Challenges to Accuracy of Student Data**: District shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Personally Identifiable Information contained in the related student's Education Records and correct erroneous information, consistent with the functionality of Services. Contractor shall cooperate and respond within thirty (30) days to the District's request for Personally Identifiable Information contained in the related student's Education Records held by the Contractor to view or correct as necessary. In the event that a parent/legal guardian of a student or other individual contacts the Contractor to review any of the Education Records or Student Data accessed pursuant to the Services, the Contractor shall refer the parent or individual to the District who will follow the necessary and proper procedures regarding the requested information, provided however, that Contractor may also allow for direct access requests (but not correction or deletion rights) of Student Data and/or Education Records from a verified parent.

E. **Security and Storage**: The District and the Contractor hereby agree that the Student Data and/or Principal or Teacher Data (if applicable) shall be stored in the following manner: Contractor agrees to employ administrative, physical, and technical safeguards consistent with industry standards designed to protect Student Data and/or Teacher Data (if applicable) from unauthorized access, disclosure, use or acquisition by an unauthorized person, including when transmitting and storing such information. Contractor will not materially decrease the overall security of the Services during the term of the Agreement. The general security duties of Contractor are set forth below. Please see Contractor's Security Whitepaper for more details: https://code.org/about/InformationSecurityPolicy.pdf .

These measures shall include, but are not limited to:

- **Passwords and Employee Access**. Contractor 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.

Contractor shall only provide access to Student Data to employees, contractors or Service Providers that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Data shall pass criminal background checks in compliance with state and local ordinances.

- **Security Protocols**. Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any Student Data, including ensuring that Student Data may only be viewed or accessed by parties legally allowed to do so. Contractor shall maintain all Student Data obtained or generated pursuant to the Agreement in a secure computer environment and not copy, reproduce, or transmit Student Data obtained pursuant to the Agreement except as necessary to fulfill the purpose of data requests by District or as otherwise set forth in the Agreement. The foregoing does not limit the ability of the Contractor to allow any necessary Service Providers to view or access data as set forth in the DPA.
- **Employee Training**. The Contractor shall provide periodic security training to those of its employees who operate or have access to the Services.
- **Security Technology**. When the Service is accessed using a supported web browser, the Provider will ensure that Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect Student Data from unauthorized access. The security measures employed shall include server authentication and data encryption at rest and in transit.. Provider shall host Student Data pursuant to the Agreement in an environment using a firewall that is periodically updated according to industry standards..
- **Periodic Risk Assessment**. Contractor further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.
- **Backups.** Contractor agrees to maintain backup copies 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.