Supplemental Agreement between the

Hewlett-Woodmere Union Free School District

And

Accurate Investigative Services Inc.

Supplemental Agreement dated this 1st day of July 2022 between the Hewlett-Woodmere Union Free School District (the "District"), located at One Johnson Place, Woodmere, NY 11598, and Accurate Investigative Services Inc. (the "Contractor") located at 28 Second Street, Athens, NY 12015.

WHEREAS, the District and Contractor have entered into a contract or other written agreement (hereinafter the "Agreement") whereby the Contractor may receive Student Data or Teacher or Principal Data, as those terms are defined in Education Law §2-d and 8 NYCRR 121.1; and

WHEREAS, the District and Contractor wish to enter into an agreement in order to comply with Education Law §2-d and 8 NYCRR Part 121 (hereinafter "Supplemental Agreement").

NOW THEREFORE, in consideration of the mutual promises below, the District and Contractor agree as follows:

1. Defined Terms: Unless otherwise indicated below or elsewhere in this Supplemental Agreement, all capitalized terms shall have the meanings provided in Education Law §2-d and Section 121.1 of the Regulations of the Commissioner of Education (hereinafter "Regulations").

a. "Educational Agency" shall generally have the same meaning as the term Educational Agency at Education Law §2-d(1)(c) and Section 121.1(f), and in reference to the party to this Agreement shall mean the Hewlett-Woodmere Union Free School District.

b. "Third Party Contractor" shall mean any person or entity, other than an Educational Agency, that receives Student Data or Teacher or Principal Data from an Educational Agency pursuant to a contract or other written agreement for purposes of providing services to such Educational Agency, including but not limited to data management or storage services, conducting studies for or on behalf of such Educational Agency, or audit or evaluation of publicly funded programs. With reference to this agreement, "Third Party Contractor" shall be synonymous with "Contractor" and shall also include any and all subcontractors, persons or entities with whom the Contractor shares Student Data and/or Principal or Teacher Data pursuant to a contract or other written agreement for purposes of providing services to such Educational Agency, including but not limited to data management or storage services, conducting studies for or on behalf of such Educational Agency, or audit or evaluation of publicly funded programs.

c. "Student" means any person attending or seeking to enroll in an Educational Agency.

d. "Student Data" means Personally Identifiable Information of a "Student."

e. "Eligible Student" means a Student who is eighteen years or older.

f. "Parent" means a parent, legal guardian, or personal in parental relation to a Student.

g. "Building Principal" or "Principal" means a building principal subject to annual performance evaluation review under Education Law §3012-c.

h. "Classroom Teacher" or "Teacher" means a teacher subject to annual performance evaluation review under Education Law §3012-c.

i. "Teacher or Principal Data" means Personally Identifiable Information from the records of an Educational Agency 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.

j. "Personally Identifiable Information" shall have the following meanings:

i. As applied to Student Data, shall mean Personally Identifiable Information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA)

ii. As applied to Teacher or Principal Data, shall mean Personally Identifiable Information as that term is defined in Education Law §3012-c.

2. The District has developed the Parents Bill of Rights for Data Privacy and Security, the terms of which are applicable to the Agreement between the District and Contractor and are incorporated into this Supplemental Agreement. The Parents Bill of Rights for Data Privacy and Security states:

Pursuant to New York State Education Law §2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information, as defined by Education Law §2-d. The Hewlett-Woodmere Public School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. This document contains a plain-English summary of such rights.

1. Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.

2. A student's personally identifiable information cannot be sold or released for any commercial or marketing purposes by the District or any a third party contractor. The district will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by the district in accordance with district policy;

3. Parents have the right to inspect and review the complete contents of their child's educational records maintained by the Hewlett-Woodmere Public Schools. (for more information about how to exercise this right, see 5500-R);

4. State and Federal Laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable student information. Safeguards associated with industry standards and best practices, including, but not limited to, encryption, firewalls, and password protection must be in place when data is stored or transferred;

5. A complete list of all student data elements collected by New York State is available for review at the following website:

    a. http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx

6. The list may also be made available by writing to:

    Chief Privacy Officer
    New York State Education Department
    89 Washington Avenue
    Albany, NY 12234

7. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

    Assistant Superintendent for Teaching, Learning, and Technology
    Hewlett-Woodmere Public Schools
    1 Johnson Place
    Woodmere, New York 11598
    (516) 792-4802

    OR

    Complaints can also be directed to the New York State Education Department online at http://nysed.gov.data-privacy-security, by mail to the

    Chief Privacy Officer
    New York State Education Department
    89 Washington Avenue
    Albany, NY 12234

    Email: privacy@mail.nysed.gov

Telephone at 518-474-0937

8. Parents have the right to be notified in accordance to applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

9. Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.

10. In the event that the District engages a third-party provider to deliver student educational services, the contractor or subcontractor will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting

    Amanda Kavanagh
    Data Protection Officer
    Hewlett-Woodmere Public Schools
    1 Johnson Place
    Woodmere, New York 11598
    (516) 792-4892
    akavanagh@hewlett-woodmere.net

    or can access the information on the District's website:
    https://www.hewlett-woodmere.net/Page/11125

Each contract with a third-party contractor which will receive student data, or teacher or principal data will include information addressing the following:

a. The exclusive purposes for which the student data or teacher or principal data will be used.

b. How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements.

c. When the agreement expires and what happens to the student data or teacher and principal data upon expiration of the agreement.

d. If and how a parent, student, a student over eighteen years of age, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

e. Where the student data or teacher or principal data will be stored, and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

7. Third-party contractors are also required to:

   a. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;

   b. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.

   c. Not use educational records for any other purpose than those explicitly authorized in the contract;

   d. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;

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

   f. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;

   g. Notify the Hewlett-Woodmere Public Schools of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;

   h. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;

   i. Provide a signed copy of this Bill of Rights to the Hewlett-Woodmere Public Schools thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

8. This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

3. As required by Education Law §2-d(3)(c) and Section 121.3 of the Regulations, the Contractor shall comply with the Data Security and Privacy Plan which is attached to this Agreement.

4. As required by Education Law §2-d(5)(e), the Contractor hereby agrees that any officers or employees of the Contractor, including any subcontractors or assignees, who have access to Student Data or Teacher or Principal Data will have or will receive training on the Federal and

New York State laws governing confidentiality of Student Data and/or Principal or Teacher Data prior to receiving access.

5. As required by Education Law §2-d(5)(f), the Contractor hereby agrees that it shall:

a. Limit internal access to education records to those individuals that are determined to have legitimate educational interests;

b. Not use the educational records for any other purposes than those explicitly authorized in the Agreement or this Supplemental Agreement;

c. Except for authorized representatives of the Contractor to the extent they are carrying out the Agreement or this Supplemental Agreement, not disclose any Personally Identifiable Information to any other party:

i. Without the prior written consent of the Parent or Eligible Student; or

ii. Unless required by statute or court order and the party provides a notice of the disclosure to the State Education Department, District Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order.

d. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;

6. Breach and unauthorized release of Personally Identifiable Information:

a. In accordance with Education Law §2-d(6) and Section 121.11 of the Regulations, the Contractor shall be required to notify the District of any breach of security resulting in an unauthorized release of Student Data and/or Principal or Teacher Data by the Contractor or its subcontractors or assignees in violation of applicable state or federal law, the Parents Bill of Rights for Student Data Privacy and Security, the data privacy and security policies of the District and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay. The District shall, upon notification by the Contractor, be required to report to the Chief Privacy Officer, who is appointed by the State Education Department, any such breach of security and unauthorized release of such data.

b. In the case of an unauthorized release of Student Data, the District shall notify the Parent or Eligible Student of the unauthorized release of Student Data that includes Personally Identifiable Information from the student records of such Student in the most expedient way possible and without unreasonable delay. In the case of an unauthorized release of Teacher or Principal Data, the District shall notify each affected Teacher or

Principal of the unauthorized release of data that includes Personally Identifiable Information from the Teacher or Principal's annual professional performance review in the most expedient way possible and without unreasonable delay.

c. In the case of notification to a Parent, Eligible Student, Teacher or Principal due to the unauthorized release of student data by the Contractor, or its subcontractors or assignees, the Contractor shall promptly reimburse the educational agency for the full cost of such notification, as required by Education Law §2-d(6)(c).

7. Miscellaneous:

a. The District and Contractor agree that if applicable laws change and/or if the Commissioner of Education implements Regulations which affects the obligations of the parties herein, this Agreement shall be deemed to incorporate such changes as necessary in order for the District and the Contractor to operate in compliance with the amendment or modified requirements under the applicable laws or regulations.

b. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the District to comply with the applicable laws or regulations.

c. Nothing express or implied in this Agreement is intended to confer upon any person other than the District, Contractor and their respective successors and assigns any rights, remedies, obligations or liabilities.

d. To the extent that any terms contained within the Contractor's terms of service, privacy policy, other policy or items similar to the foregoing conflict with the terms of this Agreement, the terms of this Agreement shall govern, supersede, and take precedence over any such conflicting terms.

IN WITNESS WHEREOF, the Parties hereto have duly executed this Agreement.

Accurate Investigative Services Inc.

By: *John A. Zimmermann*

Print Name: John A. Zimmermann

Title: Vice President

Date: 7/20/2022

HEWLETT-WOODMERE UNION FREE SCHOOL DISTRICT

By: Marie Donnelly

Print Name: Marie Donnelly

Title: ~~Assistant Superintendent~~ for Finance and Personnel

Date: Sept. 15, 2022

Data Security and Privacy Plan

As per Section 3 of the Supplemental Agreement, this plan must be completed by the Contractor.

1. Exclusive Purposes for Data Use
    a. The exclusive purposes for which the Student Data and/or Principal or Teacher Data will be used by the Contractor are as follows

The data received from your district is solely used to prepare our investigations and utilize during the course of the investigations to achieve the desired results.

Initial JAZ

2. Data Accuracy/Correction Practices
    a. Parent, student, eligible student, teacher or principal may challenge the accuracy of the data by

To challenge the accuracy of the data and/or results of the investigation, they should make a request directly with the school district, who in turn would authorize our company to provide the necessary details.

Initial JAZ

3. Security Practices
    a. The security protection taken to ensure data will be protected include [*Insert (i) a description of where Student Data and/or Principal or Teacher Data will be stored, described in a manner to protect data security, (ii) a description of the security protections taken to ensure Student Data and/or Principal or Teacher Data will be protected and data security and privacy risks are mitigated; and (iii) a description of how the Student Data and/or Principal or Teacher Data will be protected using encryption while in motion and at rest.*

Client/Student data stored locally resides on a secure server protected and monitored via a hardware firewall and security appliance with intrusion detection. Access to student information in the case management system is restricted by user role, with only management level users able to access SSN and full DOB or any HIPAA protected information. For all other users, this information is inaccessible or is redacted to prevent dissemination or storage of student data on any external devices. Policies restricting offsite storage of client/student data are in effect, and training is provided to employees regarding responsible storage and use of PII and sensitive data. Employees are prohibited by company policy from storing case data on removable devices or personal devices (SD card, thumb drive, personal smartphone, other media). All company issued devices are password protected with 2FA enabled, as well as biometric access controls.

Email communications containing client/student data use encryption to ensure security and confidentiality.

Since 2019, annual Penetration testing has been performed on our network/server in order to identify and address potential vulnerabilities and prevent intrusion. Incident Response and Disaster Recovery policies are in effect and reviewed annually.

Initial JAZ

4. Contract Lifecycle Practices
   a. The agreement expires June 30, 2023
   b. When the agreement expires, the Student Data and/or Principal or Teacher Data will be

Refer to question #3, and all data is stored for 7 years.

Initial JAZ

5. The Contractor will ensure that any and all subcontractors, persons or entities that the Contractor may share the Student Data and/or Principal or Teacher Data with will abide by the terms of the Agreement, the Supplemental Agreement, and the data protection and security requirements set forth in this Data Security and Privacy Plan, in accordance Education Law §2-d and Part 121 of the Regulations.

Initial JAZ

Accurate Investigative Services, Inc.
Company Name

John A. Zimmermann – Vice President
Print Name and Title

John A. Zimmermann 7/22/2022
Signature of Provider Date

Return to:
Amanda Kavanagh
Assistant Superintendent for Teaching, Learning, and Technology
Hewlett-Woodmere Public Schools
1 Johnson Place
Woodmere, NY 11598
akavanagh@hewlett-woodmere.net

Data Security and Privacy Plan

Question #1

The data received from your district is solely used to prepare our investigations and utilize during the course of the investigations to achieve the desired results.

Question #2

To challenge the accuracy of the data and/or results of the investigation they should request same directly with your district, who in turn would authorize our company to provide the necessary details.

Question #3

Client/Student data stored locally resides on a secure server protected and monitored via a hardware firewall and security appliance with intrusion detection.

Access to student information in the case management system is restricted by user role, with only management level users able to access SSN and full DOB or any HIPAA protected information. For all other users, this information is inaccessible or is redacted to prevent dissemination or storage of student data on any external devices. Policies restricting offsite storage of client/student data are in effect, and training is provided to employees regarding responsible storage and use of PII and sensitive data.

Employees are prohibited by company policy from storing case data on removable devices or personal devices (SD card, thumb drive, personal smartphone, other media). All company issued devices are password protected with 2FA enabled, as well as biometric access controls. Email communications containing client/student data use encryption to ensure security and confidentiality.

Since 2019, annual Penetration testing has been performed on our network/server in order to identify and address potential vulnerabilities and prevent intrusion. Incident Response and Disaster Recovery policies are in effect and reviewed annually.

Question #4

Refer to question #3 response, and all data is stored for 7 years.