DPA EXHIBIT 1 – Receiving Party's Data Privacy and Security Plan

The NYS Education Department (NYSED) is required to ensure that contracts with third-parties that receive Protected Information and/or Personally Identifiable Information (collectively, PII) include a Data Privacy and Security Plan, pursuant to Education Law § 2-d and § 121.6 of the Regulations of the Commissioner of Education. This table serves as a framework for that plan and seeks to address requirements in the law, and best practices outlined in the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **Receiving parties should not include information that could compromise the security of their data and data systems.**

1.	Outline how you will implement applicable data privacy and security contract requirements over the life of the Agreement.	Binghamton University's department of Information Security (reporting up through the Chief Information Security Officer), in conjunction with the Information Technology Research Support group, works closely with the relevant PI(s) / Data Steward(s) to monitor and control any and all regulated data on Binghamton University's campus. This includes: • Working with PI(s) to draft any relevant data use agreements • Maintaining an inventory of all regulated data on campus in a centralized repository which includes: o who may access the data, and in what capacity they may do so o Internal Data Classification Level o Dates of Previous and Upcoming Reviews o Physical and Logical Location(s) of data • Reviewing Data Use Agreements on an annual basis • Reviewing and reporting any changes which may require amendments to the DUA • Tracking any required training for all relevant parties involved in the control of regulated data sets • Reporting any data breaches (in accordance with the DUA) • Securely destroying / deleting relevant data sets at the conclusion of the research study (in accordance with the DUA)

2.	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	For the ongoing storage and access of NYSED PII data, the research team will utilize a "Google Shared Drive", (https://support.google.com/a/answer/7212025?hl=en) as configured by Binghamton University Information Technology Services Research Support Personnel, specifically for the sole use of accessing the data. Google Shared Drive is selected for this use case due to its strong level of encryption at rest as well as in transit, and the ability to tightly control user access permissions. (More information about Google Encryption: https://cloud.google.com/security/encryption-at-rest/default-encryption) The shared drive will be configured using the following settings, with the intention of limiting access of PII: • People outside Binghamton University can NOT be added to files • People who aren't shared drive members can NOT be added to files • Viewers and commenters can NOT download, print, and copy files Additionally, all users who have access to the shared drive will be configured as "Content Managers" only, such that they cannot further share documents with any users not already indicated as having access. (More information here: https://support.google.com/a/answer/7662202?hl=en) In the event that someone new requires access to the PII (or access must be revoked), the PI will submit a written request to the ITS Research Support Team via the helpdesk ticketing system (ServiceNow). At that time, ITS personnel will review the request, update the Inventory Tracking System, verify the request against the DUA, and modify the permissions accordingly. In addition, all users who are granted access to PII, must utilize Google's 2FA security (https://www.google.com/landing/2step/), and will be required to access the data from a machine which utilizes full disk encryption.

3.	Address the training received by your employees and any Subcontractors that will have access to PII.	All personnel with access to NYSED PII will be required to complete the following two training modules from the KnowBe4 platform (https://www.knowbe4.com) : **KnowBe4 Security Awareness Training** This fully interactive course takes you through two modules: Social Engineering Red Flags and Your Role*. Recognizing the tricks and techniques hackers are using against you and your organization is critical to staying safe. Join Sparr0w (a hacker) as he shares his insider knowledge and takes you behind the scenes to show you how it's done. Along the way, you'll become familiar with the signs of danger you should look for and the steps you can take to avoid becoming a victim of cybercrime. Additionally, you will practice your security awareness skills through a number of engaging scenarios. * Abridged for inclusion in the 30-minute course. **Handling Sensitive Information** This 15-minute module of the Kevin Mitnick Security Awareness Training series specializes in making sure your employees understand the importance of safely handling sensitive information, like Personally Identifiable Information (PII), Protected Health Information (PHI), Credit Card data (PCI DSS), Controlled Unclassified Information (CUI), including your organization's proprietary information and are able to apply this knowledge in their day-to-day job for compliance with regulations. A version for Canada is also available.
4.	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Agreement, at a minimum.	All Binghamton University Information Technology Services (ITS) Personnel are required to have a signed copy of the RESPONSIBLE USE / CONFIDENTIALITY AGREEMENT COMPLIANCE FORM on file: https://www.binghamton.edu/offices/human-resources/forms/pdf/hr-masters/responsible-use-agreement-form.pdf No subcontractors will be granted access to PII.

5.	Specify how you will manage any data privacy and security incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the NYSED.	In the event that the Security Operations Group has reason to believe that systems which contain CMS data have been breached, the PI/Data Steward shall be notified within 30 minutes. The PI/Data Steward will then contact NYSED within 30 minutes upon the discovery of a potential compromise to the PII data. Thus, the Data Steward / PI will notify NYSED of any suspected incidents of security with one hour of discovery. Additionally, the "University Information Security Policy" designates the Chief Information Security Officer as responsible for responding to incidents and outlines the procedure for security incident management and response.
6.	Describe how data will be transitioned to NYSED when no longer needed by you to meet your contractual obligations, if applicable.	*Please advise if this is needed for this request.*
7.	Describe your secure destruction practices and how certification will be provided to the NYSED.	The utilization of Google Shared Drives imposes Google's secure deletion practices on the NYSED PII stored within that framework: https://cloud.google.com/security/deletion Google Utilizes a 3-stage deletion approach, whereby data is marked for soft deletion, securely deleted from active systems utilizing cryptographic erasure, and then securely deleted from backup systems utilizing the cryptographic erasure methods. Binghamton University's use of Google Vault is such that once the data is logically deleted from the Shared Drive, it is still recoverable within Google Vault for 25 days thereafter. As a result, once the data is marked for deletion, the PI will notify Information Technology Services Personnel, at which point the data will be marked for deletion within Google Vault as well. Binghamton University's Chief Information Security Officer shall provide a signed letter attesting that all actions above have been completed.
8.	Outline how your data privacy and security program/practices align with NYSED's applicable policies.	Data Privacy and Security Program / practices for data covered under this agreement will adhere to PRIVACY AND