00067607.0

Addendum to Master Subscription Agreement

This Addendum ("Addendum") forms part of the Master Subscription Agreement, available at https://www.okta.com/agreements/, and incorporated herein by reference, between Okta, Inc. ("Okta") and Southern Westchester Board of Cooperative Educational Services on behalf of Lower Hudson Regional Information Center ("Customer") for the use of the Okta Service (the "Agreement"). To the extent of any conflict or inconsistency between the terms of this Addendum and the Agreement, the terms of this Addendum shall control. Any capitalized terms used in this Addendum that are not defined herein shall have the defined meaning given to them in the Agreement and the DPA.

Okta and Customer agree as follows:

1. **Parents' Bill of Rights.** Customer is responsible for using the Okta Service in compliance with the applicable requirements of the Parents' Bill of Rights for Data Privacy, attached hereto as **Attachment A**. To the extent directly applicable to Okta, Okta will also comply with the Parents' Bill or Rights for Data Privacy by complying with the terms, processes, and procedures set forth in applicable Documentation.

2. Okta shall notify Customer without undue delay but no later than seven (7) calendar days after a breach of security that causes the unlawful or accidental destruction, alteration, damage or loss, or unauthorized disclosure of or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by Okta or its Sub-processors, of which Okta becomes aware (hereinafter, a "Customer Data Incident").

IN WITNESS WHEREOF, the parties above have caused this Addendum to be signed and executed by a duly authorized person as of the date last written below.

Okta, Inc.

Accepted By: DocuSigned by: Leslie Hui 7F98ADB23206429...

Print Name: Leslie Hui

Title: VP, AO & FT

Date Signed: April 4, 2024

Customer

Accepted By: DocuSigned by: Victor Pineiro C3E40DF8437A4F0...

Print Name: Victor Pineiro

Title: Director of Technology

Date Signed: April 4, 2024

DS

okta Legal Approved

ATTACHMENT A

Parents' Bill of Rights for Data Privacy and Security

In accordance with New York State Education Law Section 2-d, the Southern Westchester Board of Cooperative Educational Services ("Southern Westchester BOCES") hereby sets forth the following Parents' Bill of Rights for Data Privacy and Security, which is applicable to all students and their parents and legal guardians.

(1) New York Stated Education law Section 2-d (Section 2-d") and the Family Educational Rights and Privacy Act ("FERPA") protect the confidentiality of personally identifiable information. Section 2-d and FERPA assure the confidentiality of records with respect to "third parties," and provides parents with the right to consent to disclosures of personally identifiable information contained in their child's education records. Exceptions to this include school employees, officials and certain State and Federal officials who have a legitimate educational need to access such records. In addition, the Southern Westchester BOCES will, upon request of parents, legal guardians or eligible students, or if otherwise required by law, disclose student records to officials of another school district in which a student seeks to enroll. An eligible student is a student who has reached 18 years of age or attends a postsecondary institution.

(2) A student's personally identifiable information cannot be sold or released for any commercial purposes;

(3) Personally, identifiable information includes, but is not limited to:

- **i.** The student's name;
- **ii.** The name of the student's parent or other family members;
- **iii.** The address of the student or student's family;
- **iv.** A personal identifier, such as the student's social security number, student number, or biometric record;
- **v.** Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
- **vi.** Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
- **vii.** Information requested by a person who the Southern Westchester BOCES reasonably believes knows the identity of the student to whom the education record relates.

(4) In accordance with FERPA, Section 2-d and Southern Westchester BOCES Policy No. 6320, Student Records: Access and Challenge, parents and legal guardians have the right to inspect and review the complete contents of their child's education record.

(5) Southern Westchester BOCES has the following safeguards in place: Encryption, firewalls and password protection, which must be in place when data is stored or transferred.

(6) New York State, through the New York State Education Department, collects a number of student data elements for authorized uses. A complete list of all student data elements collected by the State is available for public review at the following links or can be obtained by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, NY 12234: http://www.p12.nysed.gov/irs/data_reporting.html http://data.nysed.gov/ http://www.p12.nysed.gov/irs/sirs/documentation/nyssisguide. pdf

(7) Eligible students, parents and legal guardians have the right to have complaints about possible breaches of student data addressed. Any such complaint should be submitted, in writing, to the Data Protection Officer of Southern Westchester BOCES at dpo@swboces.org or at 450 Mamaroneck Avenue, Harrison, New York 10528. Parents can direct any complaints regarding possible breaches via the electronic form on the Southern Westchester BOCES home page, under Resources, and Student Privacy. The complaint form can also be found by going to https://bit.ly/swbdatabreach. Alternatively, a written complaint may also be submitted to the Chief Privacy Officer of the New York State Education Department using the form available at http://www.nysed.gov/student-data-privacy/form/reportimproper-disclosure or writing to Privacy Complaint, Chief Privacy Officer, New York State

00067607.0

Education Department, 89 Washington Avenue, Albany, New York 12234

Supplemental Information for Third-Party Contracts

In the course of complying with its obligations under the law and providing educational services, Southern Westchester BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law. Each contract the Southern Westchester BOCES enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include the following information:

Supplemental Information for the Master Subscription Agreement, available at https://www.okta.com/agreements/, between Okta, Inc. (hereinafter "Okta" or "Third-party Contractor"):

(1) the exclusive purposes for which the student data or teacher or principal data will be used:

Okta Processes Personal Data to provide its Services in accordance with the Master Subscription Agreement, which service is for identity and access management and related services pursuant to the Master Subscription Agreement.

(2) 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:

Okta conducts reasonable due diligence and security assessments of Sub-processors engaged by Okta to store and/or process Customer Data. Okta's agreement with each Sub-processor bind them to comply with applicable Data Protection Laws and Regulations and with terms no less protective of privacy and security than the provisions described below in question 5.

(3) when the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement:

Upon termination or expiration of the Master Subscription Agreement, Okta will delete Customer Data using secure deletion methods materially in accordance with applicable NIST guidelines. Customer will also have the option to obtain Customer Data in an industry-standard format prior to such deletion, as more fully described in applicable Documentation.

(4) if and 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, and:

Factoring into account the nature of the Processing, Okta shall assist Customer by appropriate organizational and technical measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

(5) where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected:

Customer Data will be hosted in secure data centers as outlined at Okta's Sub-Processor Information page. With respect to all Customer Data, Okta maintains appropriate organizational and technical measures for protection of the security, confidentiality, and integrity of Customer Data, including: logical separation of Customer Data via customer-specific IDs; role-based access privileges; a variety of configurable security controls that allow Okta customers to tailor the security of the Service for their own use; policies and procedures for identity management controls based on need-to-know criteria and the least-privilege principle; period revalidation of access privileges, unique and readily identifiable user IDs, password and other strong authentication controls; physical security policies; secure development practices; measures to detect and remediate malware, viruses and other harmful code; vulnerability management; penetration testing; intrusion, detection and prevention controls; and security breach management policies and procedures.

(6) how data will be protected using encryption while in motion and at rest:
Okta uses strong encryption to protect Customer Data in-transit and at-rest.