OK AS TO FORM
A.M.H. 2.16.2022

Data Sharing/Use Agreement

Between

Jefferson County Board of Education

And

CNXT Digital dba SchoolCNXT

This Data Sharing/Use Agreement ("Agreement") between the Jefferson County Board of Education, a political subdivision of the Commonwealth of Kentucky doing business as the Jefferson County Public Schools ("JCPS"), and CNXT Digital dba SchoolCNXT, a corporation organized under the laws of Illinois. ("Services Provider") describes the services to be provided to JCPS by Services Provider, and the means to be used by Services Provider to ensure the confidentiality and security of information and data exchanged between JCPS and Services Provider in connection with the provision of the services.

A. PERIOD OF THE AGREEMENT

This Agreement shall be effective as of March 9, 2022 and will terminate when the services contract referenced in Paragraph B.1. below terminates, unless terminated earlier by either party pursuant to Section H.

B. SCOPE OF THE AGREEMENT AND INTENDED USE OF THE DATA

1. Services Provider will provide the following services to JCPS under the terms of a services contract between JCPS and Services Provider effective March 9, 2022: providing family engagement, communication, emergency alerts and notifications delivered as a SaaS to staff, families and approved students Specific titles to be covered include: SchoolCNXT.

2. JCPS and Services Provider agree that Services Provider is an organization to which JCPS can disclose, personally identifiable information from an education record of a student, as defined in 34 CFR 99.3, under the "school official exception" of the Family Educational Rights and Privacy Act, 20 U.S.C. 1232(g) and 34 C.F.R. 99.31 (a)(1) ("FERPA"), because the disclosure is to a contractor to whom JCPS has outsourced institutional services or functions for which JCPS would otherwise use employees; the contractor is under the direct control of JCPS with respect to the use and maintenance of education records; and the contractor is subject to the requirements of 34 CFR 99.33(a) governing the use and redisclosure of personally identifiable information from education records.

3. JCPS shall disclose to Services Provider, confidential, personally identifiable information from an education record of a student, as defined in 34 C.F.R. 99.3,

under the "school official exception" of FERPA, 34 C.F.R. 99.31 (a)(1), when the disclosure is within such exception as stated in Paragraph B.2 above and Services Provider has a legitimate educational interest for access to such education records. The confidential data, including student and non-student information to be disclosed, is described in a document attached to this agreement as **Attachment A.** Services Provider shall use personally identifiable information from education records and other records in order to perform the services described in Paragraph B.1 above. Services Provider shall notify JCPS and JCPS shall provide written consent, if approved, of any changes to the list of disclosed data necessary for the services or any changes to the scope, purpose or duration of the services themselves. Any agreed upon changes to the data disclosed shall be reduced to writing and included in an update to Attachment A to this Agreement. Any agreed upon changes to the scope, purpose or duration of the services shall be reduced to writing and included in an amendment to the services contract described in Paragraph B.1 above.

4. Services Provider and JCPS shall work cooperatively to determine the proper medium and method for the transfer of confidential data between each other. Services Provider shall confirm the transfer of confidential data and notify JCPS as soon as practicable of any discrepancies between the actual data transferred and the data described in this Agreement. The same protocol shall apply to any transfer of confidential data from Services Provider to JCPS.

C. CONSTRAINTS ON USE OF DATA

1. Services Provider agrees that the services shall be provided in a manner that does not permit personal identification of parents and students by individuals other than representatives of Services Provider that have legitimate interests in the information.

2. Services Provider will not contact the individuals included in the data sets without obtaining advance written authorization from JCPS.

3. Services Provider shall not re-disclose any individual–level data with or without identifying information to any other requesting individuals, agencies, or organizations without prior written authorization by JCPS.

4. Services Provider shall use the data only for the purpose described in Paragraph B.1 above. The data shall not be used for personal gain or profit.

D. DATA CONFIDENTIALITY AND DATA SECURITY

Services Provider agrees to the following confidentiality and data security statements:

1. Services Provider acknowledges that the data is confidential data and proprietary to JCPS, and agrees to protect the data from unauthorized disclosures and to comply with all applicable Local, State and Federal confidentiality laws and regulations including but not limited to FERPA; the Kentucky Family Educational

Rights and Privacy Act, KRS 160.700 et seq.; the Richard B. Russell National School Lunch Act, 42 U.S.C. 1751 et seq.; the Child Nutrition Act of 1966, 42 U.S.C. 1771 et seq.; 7 C.F.R. 245.6 et seq.; the Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931 et seq.; and the Kentucky Open Records Act, KRS 61.820 et seq.

2. If the performance of this Agreement involves the transfer by JCPS to Services Provider of any data regarding any JCPS student that is subject to FERPA, Services Provider agrees to:

    a. In all respects comply with the provisions of FERPA.

    b. Use any such data for no purpose other than to fulfill the purposes of the services contract described in Paragraph B.1 above, and not share any such data with any person or entity other than Services Provider and its employees, contractors and agents, without the prior written approval of JCPS.

    c. Require all employees, contractors and agents of Services Provider to comply with all applicable provisions of FERPA with respect to any such data.

    d. Maintain any such data in a secure computer environment, and not copy, reproduce or transmit any such data expect as necessary to fulfill the purposes of the services contract described in Paragraph B.1 above.

    e. Provide the services under the services contract described in Paragraph B.1 above in a manner that does not permit the identification of an individual student by anyone other than employees, contractors or agents of Services Provider having a legitimate interest in knowing such personal identification.

    f. Destroy or return to JCPS any such data obtained under this Agreement within thirty days (30) after the date within it is no longer needed by Services Provider for the purposes of the services contract described in Paragraph B.1 above.

3. Services Provider shall not release or otherwise reveal, directly or indirectly, the data to any individual, agency, entity, or third party not included in this Agreement, unless such disclosure is required by law or court order. If Services Provider becomes legally compelled to disclose any confidential and otherwise personally identifiable data (whether by judicial or administrative order, applicable law, rule or regulation, or otherwise), then Services Provider shall use all reasonable efforts to provide JCPS with prior notice before disclosure so that JCPS may seek a protective order or other appropriate remedy to prevent the disclosure or to ensure JCPS's compliance with the confidentiality requirements of federal or state law; provided, however, that Services Provider will use all reasonable efforts to maintain the confidentiality of confidential and otherwise

personally identifiable data. If a protective order or other remedy is not obtained prior to the deadline by which any legally compelled disclosure is required, Services Provider will only disclose that portion of confidential and otherwise personally identifiable data that Services Provider is legally required to disclose.

4. Services Provider shall not distribute, reprint, alter, sell, assign, edit, modify or create derivative works or any ancillary materials from or with the data.

5. Services Provider shall not use data shared under this Agreement for any purpose other than the services contract described in Paragraph B.1 above. Nothing in this Agreement shall be construed to authorize Services Provider to have access to additional data from JCPS that is not included in the scope of this Agreement (or addenda). Services Provider understands that this Agreement does not convey ownership of the data to Services Provider.

6. Services Provider shall take reasonable security precautions and protections to ensure that persons not authorized to view the data do not gain access to the data. Reasonable security precautions and protections include, but are not limited to:

   a. Creating, distributing, and implementing data governance policies and procedures which protect data through appropriate administrative, technical and physical security safeguards, and outline staff responsibilities for maintaining data security;

   b. Encrypting all data carried on mobile computers/devices;

   c. Encrypting data before it is transmitted electronically;

   d. Requiring that users be uniquely identified and authenticated before accessing data;

   e. Establishing and enforcing well-defined data privilege rights which restrict users' access to the data necessary for this to perform their job functions;

   f. Ensuring that all staff accessing data sign a nondisclosure statement, attached as **Attachment B**, and maintain copies of signed statements;

   g. Securing access to any physical areas/electronic devices where sensitive data are stored;

   h. Installing a firewall to permit or deny network transmissions based upon a set of rules; and

   i. Installing anti-virus software to protect the network.

7. If Services Provider receives Personal Information as defined by and in accordance with the Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq. (the "Act"), Services Provider shall secure, protect and maintain the confidentiality of the Personal Information by, without limitation, complying with all requirements applicable to "non-affiliated third parties" set forth in the Act, including but not limited to the following:

    a. "Personal Information" is defined in accordance with KRS 61.931(6) as an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

        i. An account, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;

        ii. A Social Security number;

        iii. A taxpayer identification number that incorporates a Social Security number;

        iv. A driver's license number, state identification card number or other individual identification number issued by an agency;

        v. A passport number or other identification number issued by the United States government; or

        vi. Individually Identifiable Information as defined in 45 C.F.R. sec. 160.013 (of the Health Insurance Portability and Accountability Act), except for education records covered by FERPA.

    b. As provided in KRS 61.931(5), a "non-affiliated third party" means any person or entity that has a contract or agreement with an agency and receives (accesses, collects or maintains) personal information from the agency pursuant to the contract or agreement.

    c. Services Provider shall not re-disclose, without the written consent of JCPS, any "personal information," as defined in KRS 61.931, or any other personally identifiable information of a student or other persons, such as employees.

    d. Services Provider agrees to cooperate with JCPS in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.

e. Services Provider agrees to undertake a prompt and reasonable investigation of any breach as required by KRS 61.933.

8. If Services Provider is a cloud computing service provider (as defined in KRS 365.734(1)(b) as "any person other than an educational institution that operates a cloud computing service"), Services Provider agrees that:

    a. Services Provider shall not process student data for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services, unless the provider receives express permission from the student's parent. Services Provider shall work with the student's school and district to determine the best method of collecting parental permission. KRS 365.734 defines "process" and "student data."

    b. Pursuant to KRS 365.734(2), Services Provider shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purposes.

    c. Pursuant to KRS 365.734(2), Services Provider shall not sell, disclose, or otherwise process student data for any commercial purpose.

    d. Pursuant to KRS 365.734(3), Services Provider shall certify in writing to the agency that it will comply with KRS 365.734(2).

9. Services Provider shall report all known or suspected breaches of the data, in any format, to Dr. Kermit Belcher, Chief Information Officer. The report shall include (1) the name, job title, and contact information of the person reporting the incident; (2) the name, job title, and contact information of the person who discovered the incident; (3) the date and time the incident was discovered; (4) the nature of the incident (e.g. system level electronic breach, an electronic breach of one computer or device, a breach of hard copies of records, etc.); (5) a description of the information lost or compromised; (6) the name of the electronic system and possible interconnectivity with other systems; (7) the storage medium from which information was lost or compromised; (8) the controls in place to prevent unauthorized use of the lost or compromised information; (9) the number of individuals potentially affected; and (10) whether law enforcement was contacted.

10. Services Provider shall securely and permanently destroy the data, and any and all hard and soft (electronic) copies thereof, upon the termination of this Agreement. Services Provider agrees to require all employees, contactors, or agents of any kind using JCPS data to comply with this provision. Services Provider agrees to document the methods used to destroy the data, and upon request, provide certification to JCPS that the data has been destroyed.

11. For purposes of this agreement and ensuring Services Provider's compliance with the terms of this Agreement and all application of the state and Federal laws, Services Provider designates Paul Caliandro (or an alternative designee

specified in writing) as the temporary custodian ("Temporary Custodian") of the data that JCPS shares with Services Provider. JCPS will release all data and information under this Agreement to Temporary Custodian. Temporary Custodian shall be responsible for transmitting all data requests and maintain a log or other record of all data requested and received pursuant to this Agreement, including confirmation of the return or destruction of the data as described below. JCPS or its agents may, upon request, review the records Services Provider is required to keep under this Agreement.

12. Services Provider acknowledges that any violation of this Agreement and/or the provisions of FERPA or accompanying regulations related to the nondisclosure of protected student information constitutes just cause for JCPS to immediately terminate this Agreement.

13. Services Provider shall maintain, during the term of this Agreement, a cyber-insurance liability policy, in the amount of $5M. Upon request, Services Provider shall furnish the certificate of insurance evidencing this coverage. The certificate of insurance shall name the Board of Education of Jefferson County as additional insured in the Description of Operations section of the Certificate of Insurance which shall read:

    Board of Education of Jefferson County
    Attn: Insurance/Real Estate Dept.
    3332 Newburg Road
    Louisville, Kentucky 40218

14. Services provider shall maintain, during the term of this Agreement, ISO27001 or SOC2 certification. If Services Provider is unable to provide ISO27001 or SOC2 certification, minimum requirements on a JCPS-provided standardized questionnaire must be met. Upon request, Services Provider shall furnish a current ISO27001, SOC2 certification, or updated questionnaire.

E. FINANCIAL COSTS OF DATA-SHARING

Each party shall be responsible for their portion of costs that may result from data sharing. Examples of potential costs to JCPS are costs associated with the compiling of student data requested under this agreement and costs associated with the electronic delivery of the student data to Services Provider.

No payments will be made under this Agreement by either party. Any payments to Services Provider will be made under the services contract described in Paragraph B.1 above.

F. OBLIGATIONS OF JCPS

During the term of this Agreement, JCPS shall:

1. Prepare and deliver the data described in **Attachment A**.

G. LIABILITY

Services Provider agrees to be responsible for and assumes all liability for any claims, costs, damages or expenses (including reasonable attorneys' fees) that may arise from or relate to Services Provider's intentional or negligent release of personally identifiable student, parent or staff data ("Claim" or "Claims"). Services Provider agrees to hold harmless JCPS and pay any costs incurred by JCPS in connection with any Claim. The provisions of this Section shall survive the termination or expiration of this Agreement.

H. TERMINATION

1. This Agreement may be terminated as follows, after notification via the United States Postal Service (certified mail or registered mail) or recognized overnight delivery service (e.g., UPS, DHL, or FedEx):

    a. By either party in the event of a material breach of this Agreement by another party provided however, the breaching party shall have thirty (30) days to cure such breach and this Agreement shall remain in force.

    b. By either party after thirty (30) days advance written notice to the other party, for any reason or no reason.

2. The confidentiality provisions of this Agreement shall survive the termination of this Agreement. If this Agreement is terminated by either party for material breach or for any other reason with thirty (30) days written notice, within seven (7) days of the termination the confidential information shall be returned or destroyed within seven (7) days of the termination and the Temporary Custodian shall provide JCPS confirmation of the return or destruction of the data pursuant to Paragraph D.11. If this Agreement terminates at the end of the term described in Section A, within seven (7) days after the end of the term, Services Provider shall return or destroy all confidential information and the Temporary Custodian shall provide JCPS confirmation of the return or destruction of the data pursuant to Paragraph D.11.

3. Destruction of the confidential information shall be accomplished by utilizing an approved method of confidential destruction, including but not limited to shredding, burning or certified/witnessed destruction for physical materials and verified erasure of magnetic media using approved methods of electronic file destruction.

I. PUBLICATIONS AND COPYRIGHTS

Both parties recognize that each organization may have extant work that predates this agreement. If those materials and/or data are used in the course of this work, they remain the property of the original developer. If new materials are developed during the term of the services contract described in Paragraph B.1 above, ownership and copyright of such will be governed by the terms of the services contract.

J. MODIFICATION

No waiver, alteration or modification of the provisions of this Agreement shall be binding unless in writing and mutually agreed upon. Any modifications or additions to this Agreement must be negotiated and approved by both parties.

K. QUALITY OF SERVICES

JCPS reserves the right to review Services Provider's performance under this Agreement for effectiveness in serving the specific purposes as outlined in Paragraph B.1. Failure of Services Provider to perform in a manner that meets or exceeds the quality standards for JCPS shall serve as grounds for termination of this Agreement, subject to Service Provider's right to cure under Section H.1.a. of this Agreement.

L. BREACH OF DATA CONFIDENTIALITY

Services Provider acknowledges that the breach of this agreement or its part may result in irreparable and continuing damage to JCPS for which money damages may not provide adequate relief. In the event of a breach or threatened breach of this agreement by Services Provider, JCPS, in addition to any other rights and remedies available to JCPS at law or in equity, may be entitled to preliminary and permanent injunctions to enjoin and restrain the breach or threatened breach. If the United States Department of Education's Family Policy Compliance Office determines that Services Provider has violated paragraph 34 C.F.R. 99.31(a)(6)(iii)(B), JCPS may not allow Services Provider access to personally identifiable information from its education records for at least five (5) years.

M. CHOICE OF LAW AND FORUM

This Agreement shall be governed and construed in accordance with the laws of the Commonwealth of Kentucky. Any action or Claim arising from, under or pursuant to this Agreement shall be brought in the Jefferson County, Kentucky, Circuit Court, and the parties expressly waive the right to bring any legal action or Claims in any other courts.

N. WAIVER

No delay or omission by either party in exercising any right under this Agreement shall operate as a waiver of that or any other right or prevent a similar subsequent act from constituting a violation of this Agreement.

O. SEVERABILITY

If any part of this Agreement is held to be void, against public policy or illegal, the balance remaining provisions of this Agreement shall continue to be valid and binding.

P. NOTICES

Any notices or reports by one party to the other party under this Agreement shall be made in writing, to the address shown in the signature portions of this Agreement, or to such other address as may be designated in writing by one party to the other. Notices shall be effective when received if personally delivered, or three days after mailing if mailed.

Q. RELATIONSHIP OF PARTIES

JCPS is not an employee, agent, partner or co-venturer of or with Services Provider. Neither Services Provider nor JCPS shall represent or imply to any party that it has the power or authority to enter into a contract or commitment in the name of or on behalf of the other, or to otherwise bind the other.

R. ENTIRE AGREEMENT; ASSIGNMENT

This Agreement, together with any attachments hereto and any amendment or modifications that may hereafter be agreed to, constitute the entire understanding between the parties with respect to the subject-matter hereof and supersede any and all prior understandings and agreements, oral and written, relating hereto. Services Provider shall not assign this Agreement or any portion thereof to a subcontractor or other third party without the prior written consent of JCPS, and any attempted assignment without such prior written consent in violation of this Section R shall automatically terminate this Agreement.

AGREED:

SchoolCNXT
1920 S Highland Ave, Suite 102
Lonbard, IL 60148

BY: Paul Caliandro

Name: Paul Caliandro

Title: CIO, Chief Strategy Officer

Date: 25 Jan 2022

AGREED:

Jefferson County Board of Education
3332 Newburg Road
Louisville KY 40218

BY: ______________________________

Name: Martin A. Pollio, Ed. D.,

Title: Superintendent

Date: ______________________________

Attachment A

CONFIDENTIAL INFORMATION TO BE DISCLOSED

SchoolCNXT Data Import

Version 1.6 (May 1, 2017)

This document describes the seven files that are used to import data into the SchoolCNXT system. Those seven files are:

1. District
2. School
3. Student
4. Staff
5. Section *(optional)*
6. Section_Student *(optional)*
7. Section_Staff *(optional)*

Each file should be formatted according to the CSV spec (https://tools.ietf.org/html/rfc4180). A header row should be included in each file. The order of the fields does not matter. All files should use a UTF-8 encoding.
Note: currently the district.csv file is not used.

A Note on Phone Numbers

The Student and Staff files include fields for phone numbers labeled `phone1` and `phone2`. The Student file also includes similarly named fields for the student's two contacts: `contact1_phone1` and `contact1_phone2`; `contact2_phone1` and `contact2_phone2`. At least one of the phone number fields in each pair should represent a mobile number, it doesn't matter which one. The SchoolCNXT import process will automatically detect if a phone number is a mobile line or a land line and update its database accordingly.

District

The `district.csv` file will contain a single row of data which is the record for the district (root organization).

Field	Required	Format (if any)	Description
district_uid	Yes		Unique identifier for this district record
name	Yes		District name
phone			District phone number, typically a land line
address_line1			District address line 1
address_line2			District address line 2
city			District address city
state			District address state
zip			District address ZIP code
current_school_year		4-digit integer	The ending year of a school year (e.g., “2015” for the “2014-2015” school year)

Example

```
district_uid,name,phone,address_line1,address_line2,city,state,zip,current_scho
ol_year
dislX2000002041,Boston Public Schools,(617) 555-1234,2300 Washington
Street,,Roxbury,MA,02119,2015
```

School

The `school.csv` file will contain a row of data for each school in the district (organization).

Field	Required	Format (if any)	Description
school_uid	Yes		Unique identifier for this school record
district_uid	Yes		Identifier for the parent district record
name	Yes		School name
phone			School phone number, typically a land line
address_line1			School address line 1
address_line2			School address line 2
city			School address city
state			School address state
zip			School address ZIP code

Example

```
school_uid,district_uid,name,phone,address_line1,address_line2,city,state,zip
SKL1,dislX2000002041,Samuel Adams Elementary,(617) 555-6789,165 Webster
Street,East Boston,MA,02128

Notes:
The first field, school.system_id (School_UID) must exist in the database
example:henry-school-1

The district_uid must exist in the database
example:dislX2000002041 (Boston test district)
```

Student

The student.csv file will contain a row of data for each student in the district (organization).

Field	Required	Format (if any)	Description
student_uid	Yes		Unique identifier for this student record
state_id			Student state identifier
local_id			Student local identifier
school_uid	Yes		Identifier for the parent school record
last_name	Yes		Student last name
first_name	Yes		Student first name
middle_name			Student middle name
gender			Student gender
dob		m/d/yyyy	Student date of birth
yog		4-digit integer	Student year of graduation
grade_level			Student grade level
homeroom			Student homeroom
phone1			Student phone 1*
phone2			Student phone 2*
email1			Student email 1*
email2			Student email 2*
address_line1			Student address line 1
address_line2			Student address line 2
city			Student address city
state			Student address state
zip			Student address ZIP code
home_language			Student home language; this value should be one of the following: 1. A two-character code from the list

			of languages specified in ISO 639-1 2. A language name that corresponds to an ISO 639-1 code; SchoolCNXT can provide a list of these language names 3. A district-specific code that has been mapped to a ISO 639-1 code; contact your SchoolCNXT project manager for details
contact1_uid	Yes**		Unique identifier for this contact record
contact1_last_name	Yes**		Contact 1 last name
contact1_first_name	Yes**		Contact 1 first name
contact1_middle_name			Contact 1 middle name
contact1_phone1	Yes**		Contact 1 phone 1
contact1_phone2			Contact 1 phone 2
contact1_email1	Yes**		Contact 1 email 1
contact1_email2			Contact 1 email 2
contact1_address_line1			Contact 1 address line 1
contact1_address_line2			Contact 1 address line 2
contact1_city			Contact 1 address city
contact1_state			Contact 1 address state
contact1_zip			Contact 1 address ZIP code
contact2_uid	Yes**		Unique identifier for this contact record
contact2_last_name	Yes**		Contact 2 last name
contact2_first_name	Yes**		Contact 2 first name
contact2_middle_name			Contact 2 middle name
contact2_phone1	Yes**		Contact 2 phone 1
contact2_phone2			Contact 2 phone 2
contact2_email1	Yes**		Contact 2 email 1
contact2_email2			Contact 2 email 2
contact2_address_line1			Contact 2 address line 1

contact2_address_line2			Contact 2 address line 2
contact2_city			Contact 2 address city
contact2_state			Contact 2 address state
contact2_zip			Contact 2 address ZIP code

** These phone number and email address fields are for the student him/herself, not the related contact. These fields will typically be omitted for elementary and middle schools where students will not have their own SchoolCNXT account.*

*** These fields are required in the CSV file but their values may be blank/empty.*

Example

```
student_uid,state_id,local_id,school_uid,last_name,first_name,middle_name,gende
r_code,dob,yog,grade_level,homeroom,phone1,phone2,email1,email2,address_line1,a
ddress_line2,city,state,zip,home_language,contact1_uid,contact1_last_name,conta
ct1_first_name,contact1_middle_name,contact1_phone1,contact1_phone2,contact1_em
ail1,contact1_email2,contact1_address_line1,contact1_address_line2,contact1_cit
y,contact1_state,contact1_zip,contact2_uid,contact2_last_name,contact2_first_na
me,contact2_middle_name,contact2_phone1,contact2_phone2,contact2_email1,contact
2_email2,contact2_address_line1,contact2_address_line2,contact2_city,contact2_s
tate,contact2_zip
STU000001,10227000,8966,SKL1,Smith,John,Roger,M,1/1/2000,2018,09,203,(617)
555-9999,(781)
555-4321,jsmith18@student.bostonpublicschools.org,johnny_roger@gmail.com,100
Everett Street,Apartment 4A,East
Boston,MA,02128,Spanish,CONawif89,Smith,John,,(978)
555-8878,,jsmith@somecompany.com,,100 Everett Street,Apartment 4A,East
Boston,MA,02128,CONawif90,Martin,Mary,,(774)
555-9925,,mary_martin_78@yahoo.com,,100 Everett Street,Apartment 4A,East
Boston,MA,02128
```

Staff

The staff.csv file will contain a row of data for each staff member in the district (organization). A staff member can appear in this file multiple times each with a different school. For example, a music teacher that works at two elementary schools would appear in this file twice, once with the school_uid of each school.

This file should only include staff that will be actively using SchoolCNXT.

Field	Required	Format (if any)	Description
staff_uid	Yes		Unique identifier for this staff record
state_id			Staff state identifier
local_id			Staff local identifier
school_uid	Yes		Identifier for the parent school record
last_name	Yes		Staff last name
first_name	Yes		Staff first name
middle_name			Staff middle name
title			Staff name title (e.g., “Mr.”)
gender			Staff gender
type			Staff type (e.g., “Teacher”)
department			Staff department
homeroom1			Staff homeroom 1
homeroom2			Staff homeroom 2
phone1	Yes*		Staff phone 1
phone2			Staff phone 2
email1	Yes*		Staff email 1
email2			Staff email 2
admin		“Y” or “N”	Staff members that should have School Admin access in SchoolCNXT should be marked with a “Y” (for example, principals and assistant principals); regular, non-administrator staff members should be

			blank or marked with an “N”

** These fields are required in the CSV file but their values may be blank/empty*

Example

```
staff_uid,state_id,local_id,school_uid,last_name,first_name,middle_name,title,g
ender,type,department,homeroom1,homeroom2,phone1,phone2,email1,email2,admin
STF004399,,100-00901,SKL1,Jones,Edgar,,Mr.,M,Teacher,English,203,,(617)
555-0002,,ejones@bostonpublicschools.org,N
```

Section

The `section.csv` file will contain a row of data for each section in each school's master schedule for the current school year.

Field	Required	Format (if any)	Description
section_uid	Yes		Unique identifier for this section record
school_uid	Yes		Identifier for the parent school record
course_number	Yes		Course number (not necessarily numeric)
section_number	Yes		Section number (not necessarily numeric)
description	Yes		Section description
term			Schedule term
schedule			Schedule meeting times
room			Classroom

Example

```
section_uid,school_uid,course_number,section_number,description,term,schedule,r
oom
SEC001,SKL1,505,001,Algebra II,FY,3(M-F),203
```

Section_Student

The `section_student.csv` file will contain a row of data for each student in each section (i.e., this file represents the rosters for each class).

Field	Required	Format (if any)	Description
section_student_uid	Yes		Unique identifier for this section_student record
student_uid	Yes		Identifier for the related student record
section_uid	Yes		Identifier for the related section record

Example

```
section_student_uid,student_uid,section_uid
SECSTU0001,STU000001,SEC001
```

Section_Staff

The `section_staff.csv` file will contain a row of data for each staff member teaching each section (i.e., this file represents the teachers for each class).

Field	Required	Format (if any)	Description
section_staff_uid	Yes		Unique identifier for this section_staff record
staff_uid	Yes		Identifier for the related staff record
section_uid	Yes		Identifier for the related section record
primary_teacher	Yes	"Y" or "N"	Only one record for a given staff_uid / section_uid combination should be flagged as primary ("Y"); all other records for that combination should be blank or "N"; if there is only one record for that combination then it will automatically be imported as "Y" regardless of what the source value was
teacher_role			

Example

```
section_staff_uid,staff_uid,section_uid,primary_teacher,teacher_role
SECSTF0001,STF004399,SEC001,N,Co-teacher
```

Attachment B

SERVICE PROVIDER'S EMPLOYEE NONDISCLOSURE STATEMENT

I understand that the performance of my duties as an employee or contractor of CNXT Digital, Inc. ("Services Provider") involve a need to access and review confidential information (information designated as confidential by the Jefferson County Board of Education), and that I am required to maintain the confidentiality of this information and prevent any redisclosure prohibited under applicable federal and state law. By signing this statement, I agree to the following:

- I will not permit access to confidential information to persons not authorized by Services Provider.

- I will maintain the confidentiality of the data or information.

- I will not access data of persons related or known to me for personal reasons.

- I will report, immediately and within twenty-four (24) hours to my immediate supervisor, any known or reasonably believed instances of missing data, data that has been inappropriately shared, or data taken off site to my immediate supervisor.

- I understand that procedures must be in place for monitoring and protecting confidential information.

- I understand that the Family Educational Rights and Privacy Act ("FERPA") protects information in students' education records that are maintained by an educational agency or institution or by a party acting for the agency or institution, and includes, but is not limited to the student's name, the name of the student's parent or other family members, the address of the student or student's family, a personal identifier, such as the student's social security number, student number, or biometric record, other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name, and 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.

- I understand that any unauthorized disclosure of confidential information is illegal as provided in FERPA and in the implementing of federal regulations found in 34 CFR, Part 99. The penalty for unlawful disclosure is a fine of not more than $250,000 (under 18 U.S.C. 3571) or imprisonment for not more than five years (under 18 U.S.C. 3559), or both.

- I understand and acknowledge that children's free and reduced price meal and free milk eligibility information or information from the family's application for eligibility, obtained under provisions of the Richard B. Russell National School Lunch Act (42

U.S.C. 1751 et seq) ("NSLA") or Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.) ("CNA") and the regulations implementing these Acts, is confidential information.

- I understand that any unauthorized disclosure of confidential free and reduced price lunch information or information from an application for this benefit is illegal as provided in the NSLA or the CNA and the regulations implementing these Acts, specifically 7 C.F.R 245.6. The penalty for unlawful disclosure is a fine of not more than $1,000.00 (under 7 C.F.R. 245.6) or imprisonment for up to one year (under 7 C.F.R. 245.6), or both.

- I understand that KRS 61.931 also defines "personal information" to include an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

a) An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;

b) A Social Security number;

c) A taxpayer identification number that incorporates a Social Security number;

d) A driver's license number, state identification card number, or other individual identification number issued by any agency;

e) A passport number or other identification number issued by the United States government; or

f) Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g.

- I understand that other federal and state privacy laws protect confidential data not otherwise detailed above and I acknowledge my duty to maintain confidentiality of that data as well.

- I understand that any personal characteristics that could make the person's identity traceable, including membership in a group such as ethnicity or program area, are protected.

In addition, I understand that any data sets or output reports that I may generate using confidential data are to be protected. I will not distribute to any unauthorized person any data sets or reports that I have access to or may generate using confidential data. I understand that I am responsible for any computer transactions performed as a result of access authorized by use of sign on/password(s).

Employee signature:

Paul Caliandro

Date:

25 Jan 2022