# WISCONSIN STUDENT DATA PRIVACY AGREEMENT

School District/Local Education Agency:

Hudson School District

AND

Provider:

EO Johnson Company, Inc.

Date:

May 20, 2024

This Wisconsin Student Data Privacy Agreement ("DPA") is entered into by and between the School District of Hudson (hereinafter referred to as "LEA") and EO Johnson Company, Inc. (hereinafter referred to as "Provider") on May 20, 2024. The Parties agree to the terms as stated herein.

## RECITALS

**WHEREAS,** the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated May 20, 2024 ("Service Agreement").

**WHEREAS,** in order to provide the Services described in the Service Agreement, the Provider may receive or create, and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g and 34 CFR Part 99, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

**WHEREAS,** the documents and data transferred from LEAs and created by the Provider's Services are also subject to Wisconsin state student privacy laws, including pupil records law under Wis. Stat. § 118.125 and notice requirements for the unauthorized acquisition of personal information under Wis. Stat. § 134.98; and

**WHEREAS**, for the purposes of this DPA, Provider is a school district official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

**WHEREAS**, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

**WHEREAS**, the Provider may, by signing the "General Offer of Privacy Terms" (Exhibit "E"), agree to allow other LEAs in Wisconsin the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

**NOW THEREFORE,** for good and valuable consideration, the parties agree as follows:

## ARTICLE I: PURPOSE AND SCOPE

**1. Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, and applicable Wisconsin law, all as may be amended from time to time. In performing these services, the Provider shall be considered a School District Official with a legitimate educational interest, and performing services otherwise provided by the LEA. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.

2. **Nature of Services Provided**. The Provider has agreed to provide the following digital educational products and services described below and as may be further outlined in Exhibit "A" hereto:

Document Scanning and Conversion, plus Enterprise Essentials Document Management System

3. **Student Data to Be Provided**. The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit "B".

Special Education records for active, inactive, graduated and homeschooled students

4. **DPA Definitions**. The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over term used in the Service Agreement.

## ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Propertv of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School District Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a timely manner (and no later than 30 days from the date of the request) to the LEA's request for Student Data in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit "A", Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.

4. **Third Party Request**. Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA as soon as possible in advance of a compelled disclosure to a Third Party.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA, as well as state and federal law.

## ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance**. LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, and applicable Wisconsin law.

2. **Annual Notification of Rights**. The LEA shall include a specification of criteria under FERPA for determining who constitutes a school official and what constitutes a legitimate educational interest in its Annual notification of rights.

3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

## ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, and applicable Wisconsin law.

2. **Authorized Use**. The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.

3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.

4. **No Disclosure**. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data**. Upon written request and in accordance with the applicable terms in subsection a or b, below, Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any student data; (2) erasing; or (3) otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" form, a copy of which is attached hereto as Exhibit "D". Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

a. **Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA's request to transfer data to a separate account, pursuant to Article II, section 3, above.

b. **Complete Disposal Upon Termination of Service Agreement.** Upon Termination of the Service Agreement Provider shall dispose or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, Provider shall notify LEA in writing of its option to transfer data to a separate account, pursuant to Article II, section 3, above. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.

6. **Advertising Prohibition**. Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

## ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors 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 Records shall be subject to criminal background checks in compliance with state and local ordinances.

b. **Destruction of Data**. Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, or transfer said data to LEA or LEA's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.

c. **Security Protocols**. Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.

d. **Employee Training**. The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

e. **Security Technology**. When the service is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

f. **Security Coordinator**. If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.

g. **Subprocessors Bound**. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

h. **Periodic Risk Assessment**. Provider further acknowledges and agrees to conduct digital and physical periodic (no less than annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

2. **Data Breach**. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding seventy-two (72) hours. Provider shall follow the following process:

a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

i. The name and contact information of the reporting LEA subject to this section.
ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
iv. Whether the notification was delayed because of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

c. At LEA's discretion, the security breach notification may also include any of the following:

i. Information about what the agency has done to protect individuals whose information has been breached.
ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

d. Provider agrees to adhere to all requirements in applicable state and federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.

f. Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above. If requested by LEA, Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.

g. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

## ARTICLE VI- GENERAL OFFER OF PRIVACY TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other LEA who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

## ARTICLE VII: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b), and Article II, section 3, above.

4. **Priority of Agreements**. This DPA shall govern the treatment of student data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives before:

a. **Designated Representatives**

The designated representative for the LEA for this Agreement is:

Name: Bonnie Stegmann

Title: Chief Financial & Operations Officer

Contact Information:
(715) 377-3704
stegmannbonnie@hudsonraiders.org

The designated representative for the Provider for this Agreement is:

Name: Chris Fullarton
Title: Sr. Vice President - Imaging

Contact Information:
844-342-5365
notices@eojohnson.com

b. **Notification of Acceptance of General Offer of Privacy Terms**. Upon execution of Exhibit "E", General Offer of Privacy Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, to the designated representative below.

The designated representative for notice of acceptance of the General Offer of Privacy Terms is:

Name: Amanda McCarthy
Title: Assistant Director of Teaching and Learning for Technology

Contact Information:
(715)377-3709
mccartar@hudsonraiders.org

**6. Entire Agreement**. This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

**7. Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF WISCONSIN, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.

10.**Waiver**. No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

11.**Successors Bound**. This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business.

[*Signature Page Follows*]

**IN WITNESS WHEREOF**, the parties have executed this Wisconsin Student Data Privacy Agreement as of the last day noted below.

Provider:

BY: Date: June 06, 2024

Printed Name: Chris Fullarton Title/Position: Sr. Vice President - Imaging

Local Education Agency:

BY: Date: 06/12/2024

Printed Name: Amanda McCarthy Title/Position: Asst. Director of Teaching and Learning for Tech

*Note: Electronic signature not permitted.*

# EXHIBIT "A"

## DESCRIPTION OF SERVICES

### Description of Enterprise Essentials Document Management System:

Cloud Enterprise Essentials Edition

- 100 GB of Fully Encrypted Data Storage
- 5 Named User Licenses
- Third Party Authentication Support
- HIPAA/SOC 2 Complaint Repository
- Audit Trail/Document Versioning
- Full Text Searching
- Unlimited Web Forms
- Unlimited GlobalAction Workflows
- Cloud transformation Services with 1,000 PPD
- Multiple Database Support
- Enterprise Image Xchange

### Description of Professional Services:

- Initial Build, Design, Configuration, and Installation
- Implementation, Testing, and Training
- Upload of Scanning Project Documents
- Platinum Support (Monday-Friday 8am-5pm)

### DESCRIPTION OF DOCUMENT SCANNING & CONVERSION

**SCOPE OF WORK**

| DESCRIPTION | INCHES | 15" BOX EQUIV. | FILE CARTS | EST. IMG | EST. DATA SIZE |
|---|---|---|---|---|---|
| Sp. Education – Active | 1,200 | 80 | 4.3 | 268,880 | 26 to 28 GB |
| Sp. Education – Inactive | 624 | 42 | 2.3 | 139,818 | 14 to 16 GB |
| Sp. Education – Graduates | 504 | 34 | 1.8 | 112,930 | 10 to 12 GB |
|  | **2,328** | **156** | **8.4** | **521,628** | **50 to 56 GB** |

**RECORDS DESCRIPTION**

Page Sizes: ☒ Letter Size ☐ Legal Size ☐ 11X17 Size ☐ Large Format ☐ Half-Sheets

Page Types: ☒ Standard ☐ Card-stock ☐ Fragile (onion skin) ☐ Colored Paper

Overall Page Condition: ☐ Excellent ☒ Good ☐ Fair ☐ Poor

Additional Notes:

- Active = 50 drawers X 24" each / Inactive = 26 drawers X 24" each / Graduates = 21 drawers X 24" each
- 15" Box Equivalent = total required for Document Prep (priced per 15" box)
- File Carts = used to transfer records / 276" capacity per 2-sided cart

- Est. Images = based on average of 3,621 images per 15” box (EOJ stats from previous Sp. Education scanning)
- Est. Data Size = based on average image size of 100 KB each

## PROCESSING SPECIFICATIONS

### PACKAGING / LOGISTICS

Boxes provided by: ☐ EO Johnson ☐ Customer ☐ TBD ☒ N/A
Packaging completed by: ☒ EO Johnson ☐ Customer ☐ TBD ☐ N/A
Logistics provided by: ☒ EO Johnson ☐ Customer ☐ TBD
Logistics Type: ☒ Dedicated Trip(s) ☐ Non-Dedicated Trips (scheduled with other area business)
Trip Frequency: ☐ Weekly ☐ Bi-Weekly ☐ Monthly ☒ Other ☐ TBD
Est. Round Trips: 3 Trips (Active = 2 / Inactive + Graduates = 1)
Est. Miles / Trip: 304
Records / Trip: Est. 2.1 to 4.1 file carts per trip

Additional Notes:

- File carts (2-sided / 6 shelves each) will be used to transfer records to EOJ instead of boxes
  - More time & cost effective + provides more efficient access to files for customer requests
- EOJ will provide all Logistics services – load carts / label carts / shrink wrap carts / load carts onto truck
  - Will require use of onsite elevator (records located on upper level)
- Segmented records pickups (not all records taken for processing at one time) due to high activity level
  - Trip 1 = Active (2.2 carts)
  - Trip 2 = Active (2.1 carts)
  - Trip 3 = Inactive / Graduates (4.1 carts)
- Frequency of records pickups is TBD based upon QC level selected by customer
  - Basic Level QC = estimated pickup every 5 days
  - Premium Level QC = estimated pickup every 6-7 days
- Records pickup dates will be coordinated and established with customer

### DATABASE FILE(S)

Database Files provided by Customer: ☒ Yes ☐ No ☐ N/A

Additional Notes:

- Database file(s) must be provided to EOJ by customer prior to initial records pickup
- Database file(s) must include the following required index fields:
  - Cohort (Graduation Year)
  - Name (Last, First, MI)
  - Date of Birth
- Separate database files for Active, Inactive, and Graduates in MS Excel format is preferred
- Database file(s) will be used by EOJ as follows:
  - Create barcode sheets to be inserted in each student file in Document Prep
    - Enables auto document separation and indexing
  - Reconcile data deliveries and provide an Exception Report upon project completion

### DOCUMENT PREP SERVICES

Prep Completed by: ☒ EO Johnson ☐ Customer ☐ TBD
Prep Intensity Level: ☐ Extensive ☒ Average / Moderate ☐ Basic / Simple

Document Prep Tasks:
☒ Remove pages from folders
☐ Sort or separate pages
☒ Staple/Clip removal
☒ Page Repair/Fix bent corners
☒ Cross-pile pages for color scanning
☒ Copy file folder (labels / info)
☐ Remove pages from fasteners
☐ Purge pages
☒ Taping pages 6’x6” or smaller
☒ Insert barcode sheets
☐ Cross-pile pages 11”x17” or larger
☐ Take Inventory of records

Additional Notes:

- Copy file folders = A portion of the student files include a "Access to Student Record" label that is adhered to the inside cover of the file folder
  - If this form is blank, it will be disregarded
  - If this form has information on it, the folder will be copied, and the page will be scanned
- Cross pile – Color = any pages where color is directly related to the content of the page (i.e. color-coded charts or graphs, etc.) will be cross-piled so documents can be scanned in full color
  - This excludes an pages with highlighter marker areas – these pages will be processed in black & white
- Insert barcode sheets = a numeric barcode number will be assigned to each student file
  - Used in conjunction with customer provided database file(s)
  - Barcode number value will not be included in final data output (for EOJ production use only)

## DOCUMENT SCANNING SERVICES

Scanner(s) Used: ☒ ADF Production ☐ Large Format ☐ Flatbed
Scan Type: ☐ Front Only ☒ Duplex
Resolution: ☐ 200 dpi ☒ 300 dpi ☐ 400 dpi
Bulk Scan Color: ☒ Black & White ☐ Greyscale ☐ Full Color
Auto Blank Deletions: ☒ Yes ☐ No
Auto Rotations: ☒ Yes ☐ No
Auto Separation: ☒ Yes ☐ No
Image Cleanup: ☒ Auto-Crop ☒ De-skew ☒ De-speckle ☒ Edge cleanup ☒ Noise
removal
☐ Hole punch fill

Additional Notes:

- Any color pages cross-piled in Document Prep will be scanned in full color
- During scanning, documents will be auto separated and indexed (barcode sheets inserted in Prep)

## QUALITY CONTROL SERVICES

☒ Premium Level Quality Control

1:1 page to image review (compare every page to every image) / separate job step / blank deletions / page rotations / re-scan as needed / correct all double feeds

*RISK CONSIDERATIONS: Minimal to none. Each individual page is compared (1:1) to its scanned image. All double feeds would be identified and corrected because of the 1:1 comparison*

☒ Basic Level Quality Control

Review images only at moderate pace / separate job step / blank deletions / page rotations / documents will be pulled and for any questionable image for potential rescan based on visual assessment only / double feeds will be corrected based on visual assessment only.

*RISK CONSIDERATIONS: Double-feed pages may not be identified if overlaid directly upon each other / Pages with extremely faint writing (such as pencil writing or carbon forms) that has washed out during scanning will give visual impression of an acceptable image and would potentially not be re-scanned*

☐ Minimum Level Quality Control

Review images only at brisk pace / done in scanning step / blank deletions / page rotations / documents will be pulled and for only extremely low-quality image(s) for potential rescan based on visual assessment only / double feeds will be corrected based on visual assessment only.

*RISK CONSIDERATIONS: Review of images takes place at a faster pace than Basic Level QC. Double-feed pages may not be identified if overlaid directly upon each other / Pages with extremely faint writing (such as pencil writing or carbon forms) that has washed out during scanning will give visual impression of an acceptable image and would potentially not be re-scanned*

☐ NO Quality Control

No review whatsoever after scanning / scanned images = completed images / images will include some random blank & non-rotated pages

*RISK CONSIDERATIONS: Without any quality control, finished data will contain random blank page images or non-rotated images not auto processed during bulk scanning. Any low-quality images will not be re-scanned and no double feed pages will be identified as there will be no review.*

Additional Notes:

- This proposal includes pricing for Basic Level QC with an option to upgrade to Premium Level QC
  - Separate option for each record type – customer not required to have 1 QC level for all records

**DOCUMENT INDEXING**

Indexing Overview: ☒ Automated (no hand key) ☐ Part Automated (some hand key) ☐ All hand key

| # | INDEX FIELD NAME | METHOD OF CAPTURE |
|---|---|---|
| 1 | EOJ Barcode (not included in output) | ☐ Hand key ☐ Drop-down menu<br>☒ Barcode ☐ OCR ☐ Data lookup |
| 2 | Name (Last, First, MI) | ☐ Hand key ☐ Drop-down menu<br>☐ Barcode ☐ OCR ☒ Data lookup |
| 3 | Date of Birth | ☐ Hand key ☐ Drop-down menu<br>☐ Barcode ☐ OCR ☒ Data lookup |
| 4 | Cohort (Graduation Year) | ☐ Hand key ☐ Drop-down menu<br>☐ Barcode ☐ OCR ☒ Data lookup |
| 5 | Document Type (All "Backfile") | ☐ Hand key ☐ Drop-down menu<br>☐ Barcode ☐ OCR ☒ Data lookup |

Additional Notes:

- Fully automated document indexing (barcodes + data lookup within customer database files)
- Document Type = "Backfile" (or any specific title as determined by customer)
  - Day forward scanning will consist of specific document types
  - All paper records scanned with this project will be categorized under document type of "Backfile"

**DATA OUTPUT**

Output to: ☒ Global Search (EOJ) ☐ Other Doc Man system ☒ Windows Folders / Files

Image Output: ☒ .PDF ☐ .TIF ☐ .JPG ☐ Other

Multi-Page Documents: ☒ Yes ☐ No

Custom Image Naming: ☐ Yes ☒ No

OCR (Text Searchable): ☒ Yes ☐ No ☐ TBD

Index/Metadata Output: ☒ .CSV ☐ .TXT ☐ .XML ☐ Other ☐ N/A

Additional Notes:

- Completed data output consists of:
  - Named Windows folder by record type (Active / Inactive / Graduate)
  - 1 multi-page, text searchable, custom-named PDF file per student file
    - PDF Name = Student Name_DOB_Cohort_"Backfile".pdf

Active Files
DOE, JANE_05-20-2005_2023_Backfile.pdf
DOE, JOHN_04-15-2014_2024_Backfile.pdf
Inactive Files
Graduate Files

## Data Output Example

- An indexing metadata file (.csv format) will also be created so that data can be imported into Global Search document management system if this system is implemented

### DATA DELIVERY

Data Delivery Method: ☒ Secure FTP (SFTP) ☒ Import into Doc Man system ☐ Other
Data Delivery Process: ☐ Customer download from EOJ ☐ EOJ Upload to Customer ☐ N/A ☐ TBD ☒ Other
Data Delivery Schedule: ☒ Daily ☐ Weekly ☐ Once upon completion ☒ TBD ☐ Other

Additional Notes:

- Method / Process =
  - Windows Folders + Custom Named PDF files
    - Secure FTP delivery / data downloaded by HSD or uploaded to HSD server by EOJ
  - Global Search System data delivery
    - Data imported into Global Search by EOJ IT Engineer(s)
  - Applicable to both options:
    - Customer notified when data has been delivered
    - Notification will include update of what has been processed & delivered to date
- Schedule = daily delivery of completed data (due to high activity level)
  - Data delivered morning of each business day (processed previous business day)
- Initial Data Delivery
  - A small amount of completed data will be delivered immediately upon completion of processing
  - Customer will review data to ensure complete satisfaction with image quality and indexing accuracy
  - Customer will notify EOJ of any issues that require corrective action or will give EOJ approval to proceed with full scan production for the project

### POST PROCESSING

Review Period (after data delivery): ☐ 30 Days ☐ 60 Days ☒ 90 Days ☐ Other ☐ TBD
Post Processing - Documents: ☒ Destroy Documents ☐ Return Documents ☐ TBD
Post Processing - Data: ☒ Erase All Project Data ☐ Other

Additional Notes:

- Location of Data Disclaimer
  - EO Johnson and any of its 3rd party provider(s) agree to store and process Client's data in the continental United States
    - No 3rd party data services providers are affiliated with this project. All services completed by EOJ staff within EOJ facilities
- Document Destruction – 3rd Party Disclaimer
  - EO Johnson utilizes a 3rd party service provider for Document Shredding Services
    - NAID Certified Resource Partner
    - On-site shredding at EOJ Scan Office (mobile shred truck)
    - Bi-weekly shredding of all eligible & approved records
- Destruction / Erasure process is as follows:
  - Authorization Form sent to customer as review period is near expiration
  - Customer signature approval of Authorization / submit to EOJ
  - EOJ completed destruction and erasure process when review period has expired
  - Certificate of Destruction & Erasure provided to customer

## SCAN ON DEMAND REQUEST PROCESSING

Est. Request Volume: **7-10 Requests Daily (Active Records)**
Approved Requestors: ☐ All Customer Staff ☒ Customer to provide list
Required Response: ☐ Same Day ☒ Next Day ☐ Other ☐ TBD ☒ Rush (as needed)
Nights /Weekends/Holidays: ☐ Yes ☒ No
Delivery Method: ☒ PDF sent within encrypted email ☒ Other
Additional Notes:

- Customer to provide list of all approved requestors prior to initial records pickup
- EOJ to provide instructions to all approved requestors prior to initial records pickup

## PROJECT REPORTING

Data Delivery Notifications: Sent daily after data has been delivered
Exception Reports: Sent upon project completion
Update/Summary Reports: Sent Weekly
Additional Notes:

- Report definitions
    - Data Delivery Notifications - email communication to customer that completed data has been delivered
        - Data is available for SFTP download by HSD or has been uploaded to HSD server
        - Data has been imported into Global Search system (if this system is implemented)
    - Exception Reports –Comparison of customer database to output data to identify discrepancies
        - Student Files listed in database that were not received for processing
        - Student Files that were received for processing but not in database ("add-ons")
    - Update / Summary Reports – Includes production totals, cost to date, current averages, and projected total project cost.

## PROJECT TIMELINE

Initial Records Pickup: TBD
Records Blackout Period: Records unavailable during loading and transport
Scan Production Start: TBD
Estimated Production Duration: 16-17 days (Basic QC) / 19-20 days (Premium QC)
Estimated Completion Date: TBD
Additional Notes:

- The above stated timeline is based upon Scope of Work and Specifications as stated in this document.
- See "Logistics Services" for proposed pickup schedule
- Project Timeline is subject to change based upon the following:
    - EO Johnson production schedule
    - Available resources applied to project
    - Equipment & Technology up-time
    - Any unforeseen circumstances including natural or man-made disaster or pandemic

## CUSTOMER RESPONSIBILITIES

- Re-file all Student Files into their alphabetic location prior to records pickup(s) - See "Packaging / Logistics"
- Provide Database File(s) to EOJ – See "Database File(s)"
- Provide list of approved requestors to EOJ prior to initial pickup – See "Scan-On-Demand Request Processing"
- Review and approve Initial Data Delivery – See "Data Delivery"
- Review completed data prior to expiration of review period – See "Post Processing"
- Provide approval of destroy and/or erasure authorizations upon receipt – See "Post Processing"
- Designate recipients for EOJ email communications – "See Project Reporting"
- Designate a primary contact person to whom EOJ questions can be directed as they arise during project

# EXHIBIT "B"

SCHEDULE OF DATA

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| Application Technology Meta Data | IP Addresses of users, Use of cookies etc. | x |
| | Other application technology meta data-Please specify: | x[1] |
| | | |
| Application Use Statistics | Meta data on user interaction with application | x |
| | | |
| Assessment | Standardized test scores | x |
| | Observation data | x |
| | Other assessment data-Please specify: | x |
| | | |
| Attendance | Student school (daily) attendance data | x |
| | Student class attendance data | x |
| | | |
| Communications | Online communications that are captured (emails, blog entries) | x[2] |
| | | |
| Conduct | Conduct or behavioral data | x |
| | | |
| Demographics | Date of Birth | x |
| | Place of Birth | |
| Demographics (continued) | Gender | x |
| | Ethnicity or race | x |
| | Language information (native, preferred or primary language spoken by student) | x |
| | Other demographic information-Please specify: | x |
| Enrollment | Student school enrollment | x |
| | Student grade level | x |
| | Homeroom | |
| | Guidance counselor | |
| | Specific curriculum programs | x |
| | Year of graduation | x |
| | Other enrollment information-Please specify: | |
| | | |
| Parent/Guardian Contact Information | Address | x |
| | Email | |
| | Phone | |
| | | |
| Parent/ Guardian ID | Parent ID number (created to link parents to students) | |

[1] Provider pulls metadata for certain workflow processes—all within the system.

[2] Assessment information in the course of evaluation for special education. and outside medical assessment data.

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| | | |
| Parent/ Guardian Name | First and/or<br>Last | x<br>x |
| | | |
| Schedule | Student scheduled courses | x |
| | Teacher names | x |
| | | |
| Special Indicator | English language learner information | x |
| | Low income status | |
| | Medical alerts /health data | x |
| | Student disability information | x |
| | Specialized education services (IEP or 504) | x |
| | Living situations (homeless/foster care) | x |
| | Other indicator information- Please specify: | x<br>ECSE |
| | | |
| Student Contact Information | Address | x |
| | Email | |
| | Phone | |
| | | |
| Student Identifiers | Local (School district) ID number | x |
| | State ID number | x |

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| | Vendor/App assigned student ID number | x |
| | Student app username | |
| | Student app passwords | |
| | | |
| Student Name | First and/or<br>Last | x<br>x |
| | | |
| Student In App Performance | Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level) | x |
| | | |
| Student Program Membership | Academic or extracurricular activities a student may belong to or participate in | x |
| | | |
| Student Survey Responses | Student responses to surveys or questionnaires | |
| | | |
| Student work | Student generated content; writing, pictures etc. | x |
| | Other student work data - Please specify: | |
| | | |

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| Transcript | Student course grades | x |
| | Student course data | |
| | Student course grades/performance scores | |
| | Other transcript data -Please specify: | |
| Transportation | Student bus assignment | |
| | Student pick up and/or drop off location | |
| | Student bus card ID number | |
| | Other transportation data -Please specify: | x<br>Specialized transport |
| | | |
| Other | Please list each additional data element used, stored or collected by your application | |

No Student Data Collected at this time ______.
*Provider shall immediately notify LEA if this designation is no longer applicable.

OTHER: Use this box, if more space needed

This data is included and stored but not being collected.

## EXHIBIT "C"

## DEFINITIONS

**De-Identifiable Information (DII):** De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

**Educational Records**: Educational Records are official records, files and data directly related to a student and maintained by the school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs. For purposes of this DPA, Educational Records are referred to as Student Data.

**NIST**: Draft National Institute of Standards and Technology ("NIST") Special Publication Digital Authentication Guideline.

**Operator:** The term "Operator" means the operator of an Internet Website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Service Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in applicable state statutes.

**Personally Identifiable Information (PII):** The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

**Provider:** For purposes of the Service Agreement, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

**Pupil Generated Content:** The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

**Pupil Records:** Means all of the following: (1) Any information that directly relates to a pupil that is maintained by LEA;(2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee; and any information that meets the definition of a "pupil record" under Wis. Stat. § 118.125(1)(d). For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

**Service Agreement**: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

**School District Official**: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B) and Wis. Stat. § 118.125(2)(d), a School District Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees;
(2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) and Wis. Stat. § 118.125(2) governing the use and re-disclosure of personally identifiable information from student records.

**Student Data:** Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of Wisconsin and federal laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

**SDPC (The Student Data Privacy Consortium):** Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

**Student Personal Information:** "Student Personal Information" means information collected through a school service that personally identifies an individual student or other information collected and maintained about an individual student that is linked to information that identifies an individual student, as identified by Washington Compact Provision 28A.604.010. For purposes of this DPA, Student Personal Information is referred to as Student Data.

**Subscribing LEA:** An LEA that was not party to the original Services Agreement and who accepts the Provider's General Offer of Privacy Terms.

**Subprocessor:** For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

**Targeted Advertising**: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

**Third Party**: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

## EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

School District of Hudson directs E.O. Johnson Company, Inc. to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

| | |
|---|---|
| **Extent of Disposition**<br>Disposition shall be: | _____Partial. The categories of data to be disposed of are as follows:<br>X____Complete. Disposition extends to all categories of data. |
| | |
| **Nature of Disposition**<br>Disposition shall be by: | X____Destruction or deletion of data.<br>_____Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred, Provider shall destroy or delete all applicable data. |
| | |
| **Timing of Disposition**<br>Data shall be disposed of by the following date: | X____ At the direction of the school district when no longer under contract.<br>_____ By (Insert Date) ______________________<br>[Insert or attach special instructions] |

________________________________________ 06/12/2024

Authorized Representative of LEA Date

Christopher Fullerton 06/12/2024

Verification of Disposition of Data Date
by Authorized Representative of Provider

## EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS
School District of Hudson

**1. Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and the Hudson School District and which is dated to any other LEA ("Subscribing LEA") who accepts this General Offer though its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the other LEA may also agree to change the data provided by LEA to the Provider in Exhibit "B" to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of:
(1) a material change in the applicable privacy statutes; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form.

Provider:

BY: Christopher Fullarton Date: June 06, 2024

Printed Name: Chris Fullarton Title/Position: Senior Vice President - Imaging

**2. Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

Subscribing LEA:

BY:______________________________ Date:______________________________

Printed Name:________________________ Title/Position:______________________

**TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW**

**Name:**______________________________

**Title:**______________________________

**Email Address:** ______________________________________________

## EXHIBIT "F"

## DATA SECURITY REQUIREMENTS

No additional data security requirements specified by the parties.