

This Confidential Data Privacy Agreement (“**DPA**”) is entered into by and between:

THE BOARD OF EDUCATION OF JEFFERSON COUNTY KENTUCKY, a political subdivision of the Commonwealth of Kentucky, with its principal place of business at 3332 Newburg Road, Louisville, Kentucky 40218 (the “**Board**” or “**Jefferson County Public Schools**”) and

Canva US, Inc. a corporation organized under the laws of Delaware with its principal place of business located at 200 E. 6<sup>th</sup> Street, Austin, TX 78701 (the “**Provider**”).

**WHEREAS**, the Provider is providing educational or digital services to the Board.

**WHEREAS**, the Provider and the Board recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

**WHEREAS**, the Provider and the Board desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

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

#### ARTICLE I: PURPOSE AND SCOPE

1. **Entire Agreement.** This DPA is the entire agreement between the Parties and supersedes any and all agreements, representations, and negotiations, either oral or written, between the Parties before the effective date of this DPA. This DPA may not be amended or modified except in writing as provided below. This DPA is supplemented by the Board’s Procurement Regulations currently in effect (hereinafter “**Regulations**”) that are incorporated by reference into and made part of this DPA. In the event of a conflict between any provision of this DPA and the Regulations, the Regulations shall prevail. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
2. **Term.** This DPA shall be effective as of November 16, 2022 (the “**Effective Date**”) and shall continue for three (3) years, terminating on November 15, 2025.
3. **Services.** The services to be provided by Provider to the Board pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”). Any compensation to be provided by the Board to Provider is also detailed in **Exhibit “A”** (the “**Compensation**”). Each party shall be responsible for their portion of costs that may result from data sharing. Examples of potential costs to the Board are costs associated with the compiling of Confidential Data requested under this DPA and costs associated with the electronic delivery of Confidential DATA to Provider.
4. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Confidential Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and

performing services otherwise provided by the Board. Provider shall be under the direct control and supervision of the Board, with respect to its use of Confidential Data.

5. **Confidential Data to Be Provided.** In order to perform the Services described above, the Board shall provide Confidential Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
6. **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 terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

## ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Confidential Data Property of the Board.** All Confidential 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 Board. The Provider further acknowledges and agrees that all copies of such Confidential Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Confidential Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Confidential Data contemplated per the Service Agreement, shall remain the exclusive property of the Board. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the Board as it pertains to the use of Confidential Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the Board shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Confidential Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for the Board to respond to a parent or student, whichever is sooner) to the Board’s request for Confidential Data in a student’s records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Confidential Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the Board, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the Board, transfer, or provide a mechanism for the Board to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests.** Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Confidential Data held by the Provider pursuant to the Services, the Provider shall notify the Board in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the Board of the request.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the

Service Agreement, whereby the Subprocessors agree to protect Confidential Data in a manner no less stringent than the terms of this DPA.

6. **Research and Program Evaluation.** For any project, involving data collection or research (e.g., program evaluation or monitoring activities), student or staff participation is voluntary. As a federally authorized Institutional Review Board (IRB), the Board complies with the federal definition for research, which includes sharing of Personally Identifiable Information (PII) for the purposes of answering a question or evaluating activities for effectiveness beyond standard educational or operational procedures. Thus, all data collection and research activities must be approved by the Board's IRB and shall not begin before approval is secured from the IRB. If Provider wishes to collect data specifically for program evaluation or research purposes, or if Provider wishes to use identifiable data for program evaluation or research purposes, Provider must apply for and obtain permission from the Board's IRB prior to beginning any research or evaluation related data collection.

### ARTICLE III: DUTIES OF THE BOARD

1. **Provide Data in Compliance with Applicable Laws.** The Board shall provide Confidential Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the Board has a policy of disclosing Education Records and/or Confidential Data under FERPA (34 CFR § 99.31(a)(1)), the Board shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** The Board shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Confidential Data.
4. **Unauthorized Access Notification.** The Board shall notify Provider promptly of any known unauthorized access. The Board 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 federal, state, and local laws, rules, and regulations pertaining to Confidential Data privacy and security, all as may be amended from time to time, including but not limited to FERPA and where applicable, 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. **Data Custodian.** For the purposes of this DPA and ensuring Provider's compliance with the terms of this DPA and all application of state and federal law, Provider designated Jacqueline Davy, Head of Privacy, as the data custodian ("Data Custodian") of the Confidential Data. The Board will release all data and information under this DPA to Data Custodian. Data 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 DPA, including confirmation of the return or destruction of data as described below. The Board may, upon request, review the records Provider is required to keep under this DPA.

3. **Authorized Use.** The Confidential Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit "A"** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA. Provider will not contact the individuals included in the data sets without obtaining advance written authorization from the Board, except in the event of a data breach notification or where in response to a request from the individual.
4. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Confidential Data to comply with all applicable provisions of this DPA with respect to the Confidential Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality obligation from each employee or agent with access to Confidential Data pursuant to the Service Agreement.
5. **Insurance.** Provider shall maintain, during the term of this Agreement, a cyber-insurance liability policy, in the amount of \$5M. Upon request, Provider shall furnish the certificate of insurance evidencing this coverage.
6. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Confidential Data or any portion thereof, including without limitation, user content or other nonpublic information and/or personally identifiable information contained in the Confidential Data other than as required by law or court order. If Provider becomes legally compelled to disclose any Confidential Data (whether by judicial or administrative order, applicable law, rule, regulation, or otherwise), then Provider shall use all reasonable efforts to provide the Board with prior notice before disclosure so that the Board may seek a protective order or other appropriate remedy to present the disclosure or to ensure the Board's compliance with the confidentiality requirements of federal or state law. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Confidential Data to any third party.
7. **De-Identified Data:** Provider agrees not to attempt to re-identify De-Identified Confidential Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the Board or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive Learning purpose and for customized student Learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by the Board to return or destroy Confidential Data. Except for Subprocessors, Provider agrees not to transfer de-identified Confidential Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the Board who has provided prior written consent for such transfer. Prior to publishing any document that names the Board explicitly or indirectly, the Provider shall obtain the Board's prior written approval.
8. **Disposition of Data.** Upon written request from the Board, Provider shall dispose of or provide a mechanism for the Board to transfer Confidential Data obtained under the Service Agreement in a

usable format, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the Board is received to return the data in a usable format, Provider shall dispose of all Confidential Data after providing the Board with reasonable prior notice. The duty to dispose of Confidential Data shall not extend to Confidential Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The JCPS may employ a **“Directive for Disposition of Data”** form, a copy of which is attached hereto as **Exhibit “D”**. If the JCPS and Provider employ **Exhibit “D”**, no further written request or notice is required on the part of either party prior to the disposition of Confidential Data described in **Exhibit “D”**.

9. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Confidential Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to the Board. This section does not prohibit Provider from using Confidential Data (i) for adaptive Learning or customized student Learning (including generating personalized Learning recommendations); or (ii) to make product recommendations to teachers or JCPS employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Confidential Data as permitted in this DPA and its accompanying exhibits.
10. **Liability.** Provider agrees to be responsible for and assumes all liability for any fines, penalties, government-imposed obligations and damages awarded by a court of competent jurisdiction to the extent arising out of its intentional or negligent release of personally identifiable student, parent or staff data (“Claim” or “Claims”). Provider agrees to hold harmless the Board in connection with any Claim. The provisions of this Section shall survive the termination or expiration of this DPA.

## ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Confidential Data shall be stored within the United States. Upon request of the Board, Provider will provide a list of the locations where Confidential Data is stored.
2. **Audits.** No more than once a year, Provider will provide the Board with a copy of its annual ISO 27001 certification. The Provider will cooperate reasonably with the Board and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or the Board, and shall provide reasonable access to the Provider’s facilities, staff, agents and the Board’s Confidential Data and all records pertaining to the Provider, the Board and delivery of Services to the Board. Failure to reasonably cooperate shall be deemed a material breach of the DPA.
3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Confidential Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the standards set forth in **Exhibit “E”**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit “E”**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who the Board may contact if there are any data security concerns

or questions. Additionally, The Provider agrees to maintain a minimum security standard including but limited to the following precautions and protections:

- a) Encrypting all data, at rest and in transit;
- b) Maintaining multi-factor authentication on accounts that can access Confidential Data remotely, including 3<sup>rd</sup> party accounts;
- c) Securing access to any physical areas/electronic devices where sensitive data are stored;
- d) Establishing and enforcing well-defined data privilege rights which follow the rule of least privilege and restrict users' access to the data necessary for this to perform their job functions;
- e) Ensuring all staff and 3rd parties with access to Confidential Data are subject to an obligation of nondisclosure;
- f) Installing end-point protection including but not limited to anti-malware and anti-spyware on any device connected to the network that has access to scoped data, when applicable

4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Confidential Data that compromises the security, confidentiality or integrity of the Confidential Data maintained by the Provider the Provider shall provide notification to the Board within five (5) days of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

- (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
  - i. The name and contact information of the individual reporting a breach 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 as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
  - i. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Confidential Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- (1) 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 Confidential Data or any portion thereof, including personally identifiable information and agrees to provide the Board, upon request, with a summary of said written incident response plan.

- (2) The Board shall provide notice and facts surrounding the breach to the affected students, parents or guardians, or staff, as applicable.
- (3) In the event of a breach originating from the Board's use of the Service, Provider shall cooperate with the Board to the extent necessary to expeditiously secure Confidential Data.

**5. Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act.** If 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"), 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. 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. Provider agrees to cooperate with JCPS in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.
- e. Provider agrees to undertake a prompt and reasonable investigation of any breach as required by KRS 61.933.

6. **Cloud Computing Service Providers.** If 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"), Provider agrees that:

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. 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."

Pursuant to KRS 365.734(2), 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.

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

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

## ARTICLE VI: MISCELLANEOUS

- 7. **Termination.** Either party may terminate this DPA if the other party breaches any terms of this DPA, provided however, the breaching party shall have thirty (30) days to cure such breach and this DPA shall remain in force. The Board may terminate this DPA in whole or in part at any time by giving written notice to Provider of such termination and specifying the effective date thereof, at Least thirty (30) days before the specified effective date. In accordance with **Attachment A**, the Board shall compensate Provider for Services satisfactorily performed through the effective date of termination.
- 8. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of JCPS's Confidential Data pursuant to Article IV, section 6.
- 9. **Priority of Agreements.** This DPA shall govern the treatment of Confidential Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence.



- 10. 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.
- 11. Disputes.** Any differences or disagreements arising between the Parties concerning the rights or liabilities under this DPA, or any modifying instrument entered into pursuant to this DPA, shall be resolved through the procedures set out in the Regulations.
- 12. Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or certified mail, sent to the designated representatives below.

The designated representative for the Board for this DPA is:

Name: Dr. Kermit Belcher \_\_\_\_\_

Title: Chief Information Officer \_\_\_\_\_

Address: 3332 Newburg Rd, Louisville, KY 40218 \_\_\_\_\_

Phone: 502-485-3485 \_\_\_\_\_

Email: Kermit.belcher@jefferson.kyschools.us

The designated representative for the Provider for this DPA is:

Name: Jason Wilmot Title: Head of Education Sales

Address: 200 E. 6<sup>th</sup> Street, Austin, TX 78701

Phone: \_\_\_\_\_ Email: jwilmot@canva.com

- 13. Amendment and Waiver.** 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.
- 14. 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.
- 15. Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE COMMONWEALTH OF

KENTUCKY, 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 JEFFERSON COUNTY KENTUCKY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

- 16. 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. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the Board no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Confidential Data within the Service Agreement. The Board has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
- 17. Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Confidential Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Confidential Data and/or any portion thereof.
- 18. Relationship of Parties.** The Board is not an employee, agent, partner or co-venturer of or with Services Provider. Neither Services Provider nor the Board 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.
- 19. Equal Opportunity.** During the performance of this DPA, Provider agrees that Provider shall not discriminate against any employee, applicant or subcontractor because of race, color, national origin, age, religion, marital or parental status, political affiliations or beliefs, sex, sexual orientation, gender identity, gender expression, veteran status, genetic information, disability, or limitations related to pregnancy, childbirth, or related medical conditions. If the Compensation is paid from federal funds, this DPA is subject to Executive Order 11246 of September 24, 1965 and in such event the Equal Opportunity Clause set forth in 41 Code of Federal Regulations 60-1.4 is hereby incorporated by reference into this DPA as if set forth in full herein.
- 20. Prohibition on Conflicts of Interest.** It shall be a breach of this DPA for Provider to commit any act which is a violation of Article XI of the Regulations entitled "Ethics and Standards of Conduct," or to assist or participate in or knowingly benefit from any act by any employee of the Board which is a violation of such provisions.
- 21.** Contractor shall be in continuous compliance with the provisions of KRS Chapters 136, 139, 141, 337, 338, 341, and 342 that apply to Provider for the duration of this DPA and shall reveal any final determination of a violation by the Provider of the preceding KRS chapters.
- 22. Access to School Grounds.** No employee or agent of Provider shall access the Board's school grounds on a regularly scheduled or continuing basis for purposes of providing services to students under this DPA.

STANDARD JEFFERSON COUNTY PUBLIC SCHOOLS DATA PRIVACY AGREEMENT

Version Date:5.11.22

IN WITNESS WHEREOF, The Board and Provider execute this DPA as of the Effective Date above.

BOARD OF EDUCATION OF JEFFERSON COUNTY KENTUCKY

By: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: Martin Pollio

Title/Position: Superintendent

Canva US, Inc.

DocuSigned by:

By: Jason Wilmot Date: November 3, 2022

Printed Name: Jason Wilmot

Title/Position: Head of Education Sales

**EXHIBIT "A"**

**DESCRIPTION OF SERVICES**

Provider shall provide software licenses and support for the following products at prices equal or below Provider's standard pricing rates for the products:

Canva for Education SaaS Platform for teachers and students to design online content.

**COMPENSATION**

There shall be no cost to JCPS under this agreement. Services are provided by the Provider at no charge.

**EXHIBIT "B"**

**SCHEDULE OF DATA**

<b>Category of Data</b>	<b>Elements</b>	<b>Check if Used by Your System</b>
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	X
	Other application technology meta data Please specify:	
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	

Student class attendance data

Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Student disability information	

Category of Data	Elements	Check if Used by Your System
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	X
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	

Parent/Guardian Contact  
Information

Address

	Email	X
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	X
	Teacher names	X
Special Indicator	English language Learner information	
	Low income status	
	Medical alerts/ health data	



Category of Data	Elements	Check if Used by Your System
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Staff Data	First and Last Name	X
	Email Address	X
	Staff ID number	
	Other information – Please specify	
Student Contact Information	Address	
	Email	X
	Phone	

Student Identifiers Local (School district) ID number

	State ID number	
	Provider/App assigned student ID number	
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program  student types 60 wpm, reading program student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	X

Category of Data	Elements	Check if Used by Your System
	Other student work data -Please specify:	
Transcript	Student course grades	
	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:

Other	Please list each additional data element used, stored, or collected by your application:	
None	No Confidential Data collected at this time. Provider will immediately notify JCPS if this designation is no longer applicable.	

## **EXHIBIT “C”**

### **DEFINITIONS**

**Compensation:** Amounts to be paid to the Provider in exchange for software licenses and support. The maximum amount of Compensation that may be paid under this DPA is set forth in Attachment A. The Board is not obligated to pay the maximum Compensation amount solely by its inclusion in this DPA. Compensation owed is determined by the purchase orders submitted to Provider. The cost for any single license or support provided under this DPA shall not exceed Provider’s standard pricing for that product.

**De-Identified Data and De-Identification:** Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student’s identity is not personally identifiable, taking into account reasonable available information.

**Educational Records:** Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such 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.

**Metadata:** means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

**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 for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with the Board to provide a service to the Board shall be considered an “operator” for the purposes of this section.

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

**Regulations:** The Board Procurement Regulations, available on the JCPS website, as may be amended from time to time.

**Student Generated Content:** The term “Student-Generated Content” means materials or content created by a student in the services 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 student content.

**School Official:** For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School 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 Confidential Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

**Service Agreement:** Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

**Confidential Data:** Confidential Data includes any data, whether gathered by Provider or provided by the Board 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, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or 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, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Confidential Data includes Meta Data. Confidential Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Confidential Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Confidential Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Confidential 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.

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

**Targeted Advertising:** means presenting an advertisement to a student where the selection of the advertisement is based on Confidential Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

**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 Education Records and/or Confidential Data, as that term is used in some state statutes. However, for the purpose of this DPA, 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**

The Board of Education of Jefferson County Kentucky directs Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between The Board and Provider. The terms of the Disposition are set forth below:

**1. Extent of Disposition**

\_\_\_\_\_ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

**[Insert categories of data here]**

\_\_\_\_\_ Disposition is Complete. Disposition extends to all categories of data.

**2. Nature of Disposition**

\_\_\_\_\_ Disposition shall be by destruction or deletion of data.

\_\_\_\_\_ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

**[Insert or attach special instructions]**

**3. Schedule of Disposition**

Data shall be disposed of by the following date:

\_\_\_\_\_ As soon as commercially practicable.

\_\_\_\_\_ By **[Insert Date]**

Signature

\_\_\_\_\_  
Authorized Representative of the Board

\_\_\_\_\_  
Date

Verification of Disposition of Data

\_\_\_\_\_  
Authorized Representative of Provider

\_\_\_\_\_  
Date

**EXHIBIT “E”**

**DATA SECURITY REQUIREMENTS**

**Adequate Cybersecurity Frameworks**

Provider will utilize one of the following known and credible cybersecurity frameworks which can protect digital learning ecosystems.

Cybersecurity Frameworks

	<b>MAINTAINING ORGANIZATION/GROUP</b>	<b>FRAMEWORK(S)</b>
	American Institute of CPAs	SOC2
X	International Standards Organization (ISO)	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	The Board of Education of Jefferson County	Board provided standardized questionnaire



10 August 2022

To Whom It May Concern,

## Insurance Confirmation of Cover

### What you have told us

The following information has been used as the basis for your application for this contract of insurance. Please review the information and advise Knightcorp Insurance Brokers immediately if any of the details are incorrect or incomplete in accordance with your duty of disclosure.

<b>Policy:</b>	Public & Products Liability Insurance	
<b>Insured:</b>	Canva Inc and all subsidiaries	
<b>Insurers:</b>	HDI Global Insurance Company	
<b>Policy Numbers:</b>	GLMD5855000	
<b>Period of Insurance:</b>	30/06/2022 at 4pm to 31/05/2023 at 4pm Local Standard Time	
<b>Limit of Liability:</b>	General Aggregate Limit:	USD2,000,000 any one person or organisation
	Products-Completed Operations Aggregate Limit:	USD2,000,000 any one person or organisation
	Personal and Advertising Injury Limit:	USD2,000,000 any one person or organisation
	Each Occurrence Limit:	USD2,000,000 any one person or organisation
	Rented to you Limit:	USD1,000,000 any one premises
	Medical Expense Limit:	USD50,000 any one person

Subject at all times to the terms, conditions, definitions, exclusions & endorsements of the policy.

This confirmation of cover provides a summary of the policy cover and is current on the date of issue. It is not intended to amend, extend, replace or override the policy terms and conditions contained in the actual policy document or assume continuity of the policy beyond the expiry date noted above. This confirmation of cover is issued as a matter of information only and confers no rights upon the confirmation holder. We accept no responsibility whatsoever for any inadvertent or negligent act, error or omission on our part in preparing these statements or in transmitting this confirmation by email or for any loss, damage or expense thereby occasioned to any recipient of this document.

We will not provide any updates in relation to the policy to any third party unless we specifically agree to do so in writing with that third party.



**Andy Dyson**  
**Senior Account Manager | Corporate**



10 August 2022

To Whom It May Concern,

Insurance Confirmation of Cover

**What you have told us**

The following information has been used as the basis for your application for this contract of insurance. Please review the information and advise Knightcorp Insurance Brokers immediately if any of the details are incorrect or incomplete in accordance with your duty of disclosure.

<b>Policy:</b>	Professional Indemnity & Cyber Liability Insurance
<b>Insured:</b>	Canva Inc and all subsidiaries
<b>Insurer:</b>	Berkshire Hathaway – National Fire & Marine Insurance Company
<b>Policy Number:</b>	42-DPP-322846-01
<b>Period of Insurance:</b>	30/06/2022 at 4pm to 31/05/2023 at 4pm Local Standard Time
<b>Aggregate Limit of Liability:</b>	USD5,000,000

Subject at all times to the terms, conditions, definitions, exclusions & endorsements of the policy.

This confirmation of cover provides a summary of the policy cover and is current on the date of issue. It is not intended to amend, extend, replace or override the policy terms and conditions contained in the actual policy document or assume continuity of the policy beyond the expiry date noted above. This confirmation of cover is issued as a matter of information only and confers no rights upon the confirmation holder. We accept no responsibility whatsoever for any inadvertent or negligent act, error or omission on our part in preparing these statements or in transmitting this confirmation by email or for any loss, damage or expense thereby occasioned to any recipient of this document.

We will not provide any updates in relation to the policy to any third party unless we specifically agree to do so in writing with that third party.



**Andy Dyson**  
Senior Account Manager | Corporate



The insurance afforded herein for any subsidiary not named in this Coverage Part as a named insured does not apply to injury or damage with respect to which such insured is also a named insured under another policy or would be a named insured under such policy but for its termination or the exhaustion of its limits of insurance.

### **3. Newly Acquired Or Formed Organization**

Any organization you newly acquire or form, other than a partnership, joint venture or limited liability company, and over which you maintain financial interest of more than 50% of the voting stock, will qualify as a Named Insured if there is no other similar insurance available to that organization. However:

- a. Coverage under this provision is afforded only until the 180th day after you acquire or form the organization or the end of the policy period, whichever is earlier;
- b. Coverage **A** does not apply to "bodily injury" or "property damage" that occurred before you acquired or formed the organization; and
- c. Coverage **B** does not apply to "personal and advertising injury" arising out of an offense committed before you acquired or formed the organization.

### **4. Nonowned Watercraft**

With respect to watercraft you do not own that is less than 51 feet long and is not being used to carry persons for a charge, any person is an insured while operating such watercraft with your permission. Any other person or organization responsible for the conduct of such person is also an insured, but only with respect to liability arising out of the operation of the watercraft, and only if no other insurance of any kind is available to that person or organization for this liability.

However, no person or organization is an insured with respect to:

- a. "Bodily injury" to a co-"employee" of the person operating the watercraft; or
- b. "Property damage" to property owned by, rented to, in the charge of or occupied by you or the employer of any person who is an insured under this provision.

### **5. Additional Insureds When Required By Written Contract, Written Agreement Or Permit**

The following person(s) or organization(s) are an additional insured when you have agreed, in a written contract, written agreement or because of a permit issued by a state or political subdivision, that such person or organization be added as an additional insured on your policy, provided the injury or damage occurs subsequent to the execution of the contract or agreement.

A person or organization is an additional insured under this provision only for that period of time required by the contract or agreement.

However, no such person or organization is an insured under this provision if such person or organization is included as an insured by an endorsement issued by us and made a part of this Coverage Part.

#### **a. Vendors**

Any person(s) or organization(s) (referred to below as vendor), but only with respect to "bodily injury" or "property damage" arising out of "your products" which are distributed or sold in the regular course of the vendor's business and only if this Coverage Part provides coverage for "bodily injury" or "property damage" included within the "products-completed operations hazard".

- (1) The insurance afforded the vendor is subject to the following additional exclusions:

This insurance does not apply to:

- (a) "Bodily injury" or "property damage" for which the vendor is obligated to pay damages by reason of the assumption of liability in a contract or agreement. This exclusion does not apply to liability for damages that the vendor would have in the absence of the contract or agreement;
- (b) Any express warranty unauthorized by you;
- (c) Any physical or chemical change in the product made intentionally by the vendor;
- (d) Repackaging, except when unpacked solely for the purpose of inspection, demonstration, testing, or the substitution of parts under instructions from the manufacturer, and then repackaged in the original container;
- (e) Any failure to make such inspections, adjustments, tests or servicing as the vendor has agreed to make or normally undertakes to make in the usual course of business, in connection with the distribution or sale of the products;
- (f) Demonstration, installation, servicing or repair operations, except such operations performed at the vendor's premises in connection with the sale of the product;
- (g) Products which, after distribution or sale by you, have been labeled or relabeled or used as a container, part or ingredient of any other thing or substance by or for the vendor; or

(h) "Bodily injury" or "property damage" arising out of the sole negligence of the vendor for its own acts or omissions or those of its employees or anyone else acting on its behalf. However, this exclusion does not apply to:

(i) The exceptions contained in Sub-paragraphs (d) or (f); or

(ii) Such inspections, adjustments, tests or servicing as the vendor has agreed to make or normally undertakes to make in the usual course of business, in connection with the distribution or sale of the products.

(2) This insurance does not apply to any insured person or organization, from whom you have acquired such products, or any ingredient, part or container, entering into, accompanying or containing such products.

**b. Lessors Of Equipment**

(1) Any person(s) or organization(s) from whom you lease equipment; but only with respect to their liability for "bodily injury", "property damage" or "personal and advertising injury" caused, in whole or in part, by your maintenance, operation or use of equipment leased to you by such person(s) or organization(s).

(2) With respect to the insurance afforded to these additional insureds this insurance does not apply to any "occurrence" which takes place after the equipment lease expires.

**c. Lessors Of Land Or Premises**

Any person or organization from whom you lease land or premises, but only with respect to liability arising out of the ownership, maintenance or use of that part of the land or premises leased to you.

With respect to the insurance afforded these additional insureds the following additional exclusions apply:

This insurance does not apply to:

1. Any "occurrence" which takes place after you cease to lease that land; or
2. Structural alterations, new construction or demolition operations performed by or on behalf of such person or organization.

**d. Architects, Engineers Or Surveyors**

Any architect, engineer, or surveyor, but only with respect to liability for "bodily injury", "property damage" or "personal and advertising injury" caused, in whole or in part, by your acts or omissions or the acts or

omissions of those acting on your behalf:

(1) In connection with your premises; or

(2) In the performance of your ongoing operations performed by you or on your behalf.

With respect to the insurance afforded these additional insureds, the following additional exclusion applies:

This insurance does not apply to "bodily injury", "property damage" or "personal and advertising injury" arising out of the rendering of or the failure to render any professional services by or for you, including:

1. The preparing, approving, or failing to prepare or approve, maps, shop drawings, opinions, reports, surveys, field orders, change orders or drawings and specifications; or
2. Supervisory, inspection, architectural or engineering activities.

This exclusion applies even if the claims against any insured allege negligence or other wrongdoing in the supervision, hiring, employment, training or monitoring of others by that insured, if the "occurrence" which caused the "bodily injury" or "property damage", or the offense which caused the "personal and advertising injury", involved the rendering of or the failure to render any professional services by or for you.

**e. Permits Issued By State Or Political Subdivisions**

Any state or political subdivision, but only with respect to operations performed by you or on your behalf for which the state or political subdivision has issued a permit.

With respect to the insurance afforded these additional insureds, this insurance does not apply to:

- (1) "Bodily injury", "property damage" or "personal and advertising injury" arising out of operations performed for the state or municipality; or
- (2) "Bodily injury" or "property damage" included within the "products-completed operations hazard".

**f. Any Other Party**

Any other person or organization who is not an additional insured under Paragraphs a. through e. above, but only with respect to liability for "bodily injury", "property damage" or "personal and advertising injury" caused, in whole or in part, by your acts or omissions or the acts or omissions of those acting on your behalf:

- (1) In the performance of your ongoing operations;

