

Data Sharing/Use Agreement**Between****Jefferson County Board of Education****And*****EdjAnalytics, LLC***

This Data Sharing/Use Agreement ("Agreement") between the Jefferson County Board of Education, a political subdivision of the Commonwealth of Kentucky doing business as the Jefferson County Public Schools ("Data Provider"), and EdjAnalytics, LLC, a limited liability company organized under the laws of Kentucky ("Research Organization") describes the research project proposed by Research Organization, and the means to be used by Research Organization to ensure the confidentiality and security of information and data exchanged between Data Provider and Research Organization.

A. PERIOD OF THE AGREEMENT

This Agreement shall be effective as of **March 24, 2020** and will terminate **June 30, 2021** unless terminated earlier by either party pursuant to Section H.

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

1. SCOPE OF WORK/PROJECT DESCRIPTION – The use of data received under this agreement is limited to the purpose and scope described in Exhibit A. Only data elements included in Exhibit A will be provided to Research Organization under this Agreement.
2. Data Provider and Research Organization agree that Research Organization is an organization to which Data Provider can disclose, upon written request, personally identifiable information from an education record of a student, as defined in 34 CFR 99.3, under the "studies exception" of the Family Educational Rights and Privacy Act, 20 U.S.C. 1232(g) and 34 C.F.R. 99.31 (a)(6) ("FERPA"), because the disclosure is to conduct studies for, or on behalf of, Data Provider to: develop, validate, or administer predictive tests; administer student aid programs; or improve instruction.
3. Data Provider shall disclose to Research Organization, upon written request, confidential, personally identifiable information from an education record of a student, as defined in 34 C.F.R. 99.3, under the "studies exception" of FERPA, 34 C.F.R. 99.31 (a)(6), when the disclosure is to conduct studies for, or on behalf of, Data Provider to: develop, validate, or administer predictive tests; administer student aid programs; or improve instruction. The confidential data including student and non-student information to be disclosed is described in a document attached to this Agreement as **Exhibit A**. Research Organization shall use personally identifiable information from education records and other records in order to perform the studies described in Exhibit A. The description of the studies, as included in Exhibit A, shall include the purpose and scope of the studies, the duration of the studies, a specific description of the methodology of disclosure and an explanation as to the need for confidential data to perform these studies. Research

Organization shall notify Data Provider and Data Provider shall provide written consent, if approved, of any changes to the list of disclosed data necessary for the studies or any changes to the scope, purpose or duration of the studies themselves. Any agreed upon changes to the data disclosed or to the studies shall be reduced to writing and included in Exhibit A.

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

C. CONSTRAINTS ON USE OF DATA

1. Research Organization agrees that the research shall be conducted in a manner that does not permit personal identification of parents and students by individuals other than representatives of Research Organization that have legitimate interests in the information.
2. Research Organization will report only aggregate data and will not report any individual data, nor will data be reported in a manner that permits indirect identification of any individual.
3. Research Organization will not contact the individuals included in the data sets without obtaining advance written authorization from Data Provider.
4. Research Organization shall not re-disclose any individual – level data with or without identifying information to any other requesting individuals, agencies, or organizations without prior written authorization by Data Provider.
5. Research Organization shall use the data only for the purpose described in Exhibit A. The data shall not be used for personal gain or profit.

D. DATA CONFIDENTIALITY AND DATA SECURITY

Research Organization agrees to the following confidentiality and data security statements:

1. Research Organization acknowledges that the data is confidential data and proprietary to Data Provider, and agrees to protect the data from unauthorized disclosures and to comply with all applicable Data Provider, Local, State and Federal confidentiality laws and regulations including but not limited to FERPA; the Privacy Act of 1974, 5 U.S.C. 552a; 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.; the Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931 et seq.; the Kentucky Open Records Act, KRS 61.820 et seq.; and the California Education Code.

2. If the performance of this Agreement involves the transfer by Data Provider to Research Organization of any data regarding any Data Provider student that is subject to FERPA, Research Organization agrees to:
 - a. In all respects comply with the provisions of FERPA.
 - b. Use any such data for no purpose other than to fulfill the purposes of the Project, and not share any such data with any person or entity other than Research Organization and its employees, contractors and agents, without the approval of Data Provider.
 - c. Require all employees, contractors and agents of Research Organization to comply with all applicable provisions of FERPA with respect to any such data.
 - d. Maintain any such data in a secure computer environment, and not copy, reproduce or transmit any such data except as necessary to fulfill the purposes of the Project.
 - e. Conduct the Project in a manner that does not permit the identification of an individual student by anyone other than employees, contractors or agent of Research Organization having a legitimate interest in knowing such personal identification, and not disclose any such data in a manner that would permit the identification of an individual student in any published results of studies.
 - f. Destroy or return to Data Provider any such data obtained under this Agreement within thirty days (30) after the date within it is no longer needed by Research Organization for the purposes of the Project.
 - g. If free or reduced price lunch eligibility data (i.e., free or reduced price lunch eligibility data which is the student poverty indicator for most education programs) is to be released to the Researcher, then the Data Provider shall disclose this data to the Research Organization, upon written request utilizing the U.S. Department of Agriculture prototype request and confidentiality agreement, and upon the Data Provider agreeing that the Research organization has demonstrated that disclosure is allowed by 7 C.F.R. 245.6. A description of any data protected by 7 C.F.R 245.6 which is to be disclosed under this agreement shall be included in Exhibit A. Any agreed upon changes to the data disclosed or to the studies shall be reduced to writing and included in Exhibit A to this agreement.
3. Research Organization shall not release or otherwise reveal, directly or indirectly, the data to any individual, agency, entity, or third party not included in this Agreement, unless such disclosure is required by law or court order. If Research Organization becomes legally compelled to disclose any confidential and otherwise personally identifiable data (whether by judicial or administrative order, applicable law, rule or regulation, or otherwise), then Research Organization shall use all reasonable efforts to provide Data Provider with prior notice before disclosure so that Data Provider may seek

a protective order or other appropriate remedy to prevent the disclosure or to ensure Data Provider's compliance with the confidentiality requirements of federal or state law; provided, however, that Research Organization will use all reasonable efforts to maintain the confidentiality of confidential and otherwise personally identifiable data. If a protective order or other remedy is not obtained prior to the deadline by which any legally compelled disclosure is required, Research Organization will only disclose that portion of confidential and otherwise personally identifiable data that Research Organization is legally required to disclose.

4. Research Organization shall not distribute, reprint, alter, sell, assign, edit, modify or create derivative works or any ancillary materials from or with the data, other than publications permitted under Section I of this Agreement.
5. Research Organization shall not use data shared under this Agreement for any purpose other than the goals outlined in this Agreement. Nothing in this Agreement shall be construed to authorize Research Organization to have access to additional data from Data Provider that is not included in the scope of this Agreement (or addenda). Research Organization understands that this Agreement does not convey ownership of the data to Research Organization.
6. Research Organization shall take reasonable security precautions and protections to ensure that persons not authorized to view the data do not gain access to the data as described in **Exhibit C**. Reasonable security precautions and protections include, but are not limited to:
 - a. Creating, distributing, and implementing data governance policies and procedures which protect data through appropriate administrative, technical and physical security safeguards, and outline staff responsibilities for maintaining data security;
 - b. Encrypting all data carried on mobile computers/devices;
 - c. Encrypting data before it is transmitted electronically;
 - d. Requiring that users be uniquely identified and authenticated before accessing data;
 - e. Establishing and enforcing well-defined data privilege rights which restrict users' access to the data necessary for this to perform their job functions;
 - f. Ensuring that all staff accessing data sign a confidentiality agreement or nondisclosure statement, attached as **Exhibit B**, and maintain copies of signed confidentiality agreements or nondisclosure statements;
 - g. Securing access to any physical areas/electronic devices where sensitive data are stored;

- h. Installing a firewall to permit or deny network transmissions based upon a set of rules; and
 - i. Installing anti-virus software to protect the network.
- 7. If Research Organization 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"), Research Organization 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 the Commonwealth and receives (accesses, collects or maintains) personal information from the Commonwealth pursuant to the contract or agreement."
 - c. Research Organization shall not re-disclose, without the written consent of Data Provider, 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. Research Organization agrees to cooperate with Data Provider in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.
 - e. Research Organization agrees to undertake a prompt and reasonable investigation of any breach as required by KRS 61.933.
- 8. If Research Organization is a cloud computing service provider (as defined in KRS 365.734(1)(b) as "any person or entity other than an educational institution that operates a cloud computing service"), Research Organization agrees that:
- 9. Research Organization 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. Research Organization 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."
- 10. With a written agreement for educational research, Research Organization may assist an educational institution to conduct educational research as permitted by FERPA.
- 11. Pursuant to KRS 365.734, Research Organization 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.
- 12. Pursuant to KRS 365.734, Research Organization shall not sell, disclose, or otherwise process student data for any commercial purpose.
- 13. Pursuant to KRS 365.734, Research Organization shall certify in writing to the agency that it will comply with KRS 365.734(2).
- 14. Research Organization shall report all known or suspected breaches of the data, in any format, to Dr. Dena Dossett, Chief, Accountability, Research, and Systems Improvement. The report shall include (1) the name, job title, and contact information of the person reporting the incident; (2) the name, job title, and contact information of the person who discover the incident; (3) the date and time the incident was discovered; (4) the nature of the incident (e.g. system level electronic breach, an electronic breach of one computer or device, or a breach of hard copies of records; (5) a description of the information lost or compromised; (6) the name of the electronic system and possible interconnectivity with other systems; (7) the storage medium from which information was lost or compromised; (8) the controls in place to prevent unauthorized use of the lost or compromised information; (9) the number of individuals potentially affected; and (10) whether law enforcement was contacted.
- 15. Research Organization shall securely and permanently destroy the data, and any and all hard and soft (electronic) copies thereof, upon the termination of this Agreement as described in Exhibit D. Research Organization agrees to require all employees, contactors, or agents of any kind using Data Provider data to comply with this provision.

Research Organization agrees to document the methods used to destroy the data, and upon request, provide certification to Data Provider that the data has been destroyed.

16. For purposes of this agreement and ensuring Research Organization's compliance with the terms of this Agreement and all application of the state and Federal laws, Research Organization designates Brandon Debes (or an alternative designee(s) specified in **Exhibit D**) as the temporary custodian ("Temporary Custodian") of the data that Data Provider shares with Research Organization. Data Provider will release all data and information under this Agreement to Temporary Custodian. Temporary Custodian shall be responsible for transmitting all data requests and maintain a log or other record of all data requested and received pursuant to this Agreement, including confirmation of the return or destruction of the data as described below. Data Provider or its agents may, upon request, review the records Research Organization is required to keep under this Agreement.
17. Research Organization has the right, consistent with scientific standards, to present, publish, or use student results it has gained in the course of its analysis, but only if the publication, presentation, or use does not include personally identifiable information of parents, students, or teachers, and not outside the bounds of a research study.
18. Should Research Organization use or collect data for conducting a research study, Research Organization will separately submit an external research request through Data Provider's online system: <https://assessment.jefferson.kyschools.us/DRMS/>.
19. Should Research Organization present, publish, or use student results it has gained in the course of its analysis, Research Organization shall adhere to the following terms:
 - a. Research Organization shall not publish, present, or use reports that include a cell size of less than 10. Reports must mask these cells so that the results are not revealed.
 - b. Publications and reports of data and information shared, including preliminary descriptions and draft reports, shall involve only aggregate data and no personally identifiable information or other information that could lead to the identification of any student, parent, or teacher.
 - c. No less than fifteen (15) business days prior to public disclosure of its data analysis, Research Organization will provide Data Provider a manuscript or other draft of the proposed public disclosure. Within fifteen (15) business days following receipt thereof, Data Provider will notify Research Organization in writing if the proposed disclosure contains any confidential information and specify the portions of the proposed disclosure requiring redaction.
 - d. Research Organization shall provide Data Provider, free of charge and within thirty (30) days, a copy of any report that is generated using the data.

- e. Reports or articles based on data obtained from Data Provider under this agreement must include the following acknowledgment: “This report/article was made possible, in part, by the support of the Jefferson County, Kentucky, Public Schools. Opinions contained in this report/article reflect those of the author and do not necessarily reflect those of the Jefferson County, Kentucky, Public Schools.” Data Provider must be cited as the source of the data in all tables, reports, presentations, and papers.

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

E. FINANCIAL COSTS OF DATA-SHARING

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

No payments will be made under this agreement by either party.

F. OBLIGATIONS OF DATA PROVIDER

During the term of this Agreement, Data Provider shall:

1. Prepare and deliver student demographic and academic data as defined in **Exhibit A – Data File Description**. All items will be keyed to a “proxy” student identifier that is different from the official student ID. The link between the official and proxy IDs will not be disclosed by Data Provider. No personally identifiable information will be provided to Research Organization.
2. After the initial data is provided for the requested student population, Data Provider will not provide supplementary data for additional students.
3. Provide Data Stewardship training for data custodian.

G. LIABILITY

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

H. TERMINATION

1. This Agreement may be terminated as follows, after notification via the United States Postal Service (certified mail or registered mail) or recognized overnight delivery service (e.g., UPS, DHL, or FedEx):
 - a. By either party immediately in the event of a material breach of this Agreement by another party.
 - b. By either party after thirty (30) days advance written notice to the other party, for any reason or no reason.
2. The confidentiality provisions of this Agreement shall survive the termination of this Agreement. If this Agreement is terminated by either party for material breach or for any other reason with thirty (30) days written notice, the confidential information shall be returned or destroyed within seven (7) days of the termination. If this Agreement terminates at the end of the term described in Section A, Research Organization shall return or destroy all confidential information when it is no longer needed for the study. Such return or destruction shall occur within seven (7) days after it is no longer needed for the study.
3. Destruction of the confidential information shall be accomplished by utilizing an approved methods of confidential destruction, including shredding, burning or certified/witnessed destruction for physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. Detailed data destruction plan is provided in **Exhibit D**. Research Organization's Certificate of Data Destruction is provided in **Exhibit E**.

I. PUBLICATIONS AND COPYRIGHTS

Both parties recognize that each organization may have extant work that predates this agreement. If those materials and/or data are used in the course of this work, they remain the property of the original developer or researcher. If new materials are developed during the project, ownership and copyright of such will remain with the developing entity.

J. MODIFICATION

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

K. QUALITY OF SERVICES

Data Provider reserves the right to review Research Organization's performance under this Agreement for effectiveness in serving the specific purposes as outlined in Paragraph B.1. Failure of Research Organization to perform in a manner that meets or exceeds the quality standards for Data Provider shall serve as grounds for termination of this Agreement.

L. BREACH OF DATA CONFIDENTIALITY

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

M. CHOICE OF LAW AND FORUM

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

N. WAIVER

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

O. SEVERABILITY

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

P. NOTICES

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

Q. RELATIONSHIP OF PARTIES

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

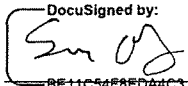
R. ENTIRE AGREEMENT; ASSIGNMENT

This Agreement, together with any attachments hereto and any amendment or modifications that may hereafter be agreed to by the constitute the entire understanding between the parties with

respect to the subject-matter hereof and supersede any and all prior understandings and agreements, oral and written, relating hereto. Research Organization shall not assign this Agreement or any portion thereof to a subcontractor or other third party without the prior written consent of Data Provider, and any attempted assignment without such prior written consent in violation of this Section R shall automatically terminate this Agreement.

AGREED:

EdjAnalytics, LLC
732 East Market Street
Louisville, KY 40202

BY:  BE11C54F6EDA4C3...

Name: Sean O'Leary

Title: CEO and Co-Founder

Date: 3/12/2020

AGREED:

Jefferson County Board of Education
3332 Newburg Road
Louisville, KY 40218

BY: _____

Name: _____

Title: _____

Date: _____

61617751.2

Description of Exhibits

To authorize the release and use of confidential data under the FERPA Studies Exception. Exhibits referenced in the Agreement must be completed and incorporated into the final Agreement.

Exhibits include:

- Exhibit A –
 - Section I – describes the study, funding source and data being requested
 - Section II – describes the need for Personally Identifiable Information (PII)
 - Section III required if requesting Free and Reduced Lunch information
- Exhibit B – Research Organization Nondisclosure Statements (one for each data custodian)
- Exhibit C – Research Organization data security policy
- Exhibit D – Data destruction plan at completion of study and identification of data custodians
- Exhibit E – Research Organization's Certificate of Data Destruction

Please refer to the U.S. Department of Education, Family Policy Compliance Office's Guidance for Reasonable Methods and Written Agreements for additional information on requirements for data sharing under the Family Education Rights and Privacy Act (FERPA).

Exhibit A

Contact Information:

Research Organization Legal Name: EdjAnalytics, LLC

Primary Data Custodian Name: Brandon Debes

Title: Database Administrator

Phone: 502-287-8257

Email: BDebes@edjanalytics.com

Secondary Data Custodian Name: Dennis Gomer

Title: Data Scientist, Director of IT

Phone: 502-225-3016

Email: DGomer@edjanalytics.com

Section I – to be completed by all requestors:

Describe purpose, scope and duration of study – use of data received under this agreement is limited to purpose and scope defined.

- Describe purpose and scope of the study.
- Describe any grant, third party or other funding source for study.
- Describe how results of study will be used and include Vision 2020 strategy supported by the study.

Please see attached: *EdjAnalytics Response, Exhibit A, Section I: Purpose, Scope and Duration*

Start Date of Study: March 24, 2020

End Date of Study: June 30, 2021

Data Being Requested – provide specific data elements needed to complete study.

Please see attached: *EdjAnalytics Response, Exhibit A, Section I: Data Being Requested*

Section II – Complete if Personally Identifiable Information (PII) is being requested:

- Justify your request for student/individual level data.
- Explain why study could not be completed using aggregate-level data without PII.

Please see attached: *EdjAnalytics Response, Exhibit A, Section II: Personally Identifiable Information (PII) Requested*

Special requirements for requests for Personally Identifiable Information (PII)

- *Student-Level/Individual detail from education records can only be used to meet the purpose or purposes of the study as stated in this MOU for duration as defined.*
- *Research Organization agrees to conduct the study in a manner that does not permit the personal identification of parents, students, individuals by anyone other than designated data custodians.*
- *Research Organization agrees to destroy all PII from education records and confidential data from other records.*

If Free/Reduced Lunch status is needed on PII, complete Section III.

EdjAnalytics Response

Exhibit A, Section I: Purpose, Scope and Duration

Purpose and Scope

Edj is proposing to support JCPS with one predictive analysis:

- 1) As stated in the 2017 Data Sharing Agreement, Edj and JCPS have a long-term vision of developing a K-12 early warning system to flag students who are not on track to meet other key milestones throughout the education journey. To support that vision, Edj will undertake a new study to identify students who are at risk of underperforming on 3rd grade reading tests. We will analyze student-specific data from pre-Kindergarten to 3rd grade to understand the drivers that predict the results of the 3rd grade reading test.

Funding

We are considering several funding options for this project. Funding is being sought from local foundations and individuals. Internal funding from Edj founders is also being considered. Funding for the study will be of no cost to the Jefferson County Public Schools system.

Results of Study

Results from this study will be used to develop the earliest warning signals available to JCPS. Identifying which students are at risk of falling behind in primary years will enable JCPS educators and staff to provide interventions which may increase the students' chances of persisting to high school graduation and beyond.

This study directly supports *Strategy 1.17 Eliminate Achievement Learning and Opportunity Gaps*, and *Vision 2020* which states *All Jefferson County Public Schools students graduate prepared, empowered, and inspired to reach their full potential and contribute as thoughtful, responsible citizens of our diverse, shared world.*

EdjAnalytics Response

Exhibit A, Section I: Data Being Requested

Grade Levels: Kindergarten to 3rd Grade

School Years: 2016-2020

Each enrollment occurrence

Field	Notes
StudentID	A proxy ID will be used.
Current SchoolID	
Current SchoolName	
Current School Type	
Student Birthdate	
Student Race	Ethnicity Federal Codes
Student Gender	
Student Current Grade	
Student Actual Grade	Used with Special Education Student
SpecialEdStatus	
LEP Indicator	English Language Learner
Language Spoken at Home	
Homeless Indicator	
Foster Care Flag	
Interrupted Schooling	
Start Status	Entry Code (Include Code Map)
End Status	Close of Year, Withdrawal or Graduate (Include Code Map)
Start Date	
End Date	
School Year	
Resides School	
Attends School	
Census Block Group	
Zip code	
Relationship	(Indicate Mother and/ or Father only)
Days Absent	
Attendance Code	Absent (Excused / Unexcused)
Suspension Indicator	Out of school Suspensions
Number of Behavior Referrals (Disciplinary Actions)	If this variable shows promise, we can share additional detail around type of disciplinary action
Early Learning Location/Type (Brigance Self-Report)	
Teacher of Record	A proxy ID will be used.
Years teaching experience in JCPS	
Term	Grading Period (every nine weeks)
Grades (O, S, NI, U)	
Number of hours of reading and math intervention	
K-Prep Scores	Data limited to 3rd grade
MAP Scores	Data limited to schools where MAP was administered; varies by yr.
Brigance Scores	Provide data available in current format
Interventions by Kentucky Family Resource & Youth Services Centers	

EdjAnalytics Response
Exhibit A, Section II: Personally Identifiable Information (PII) Requested

The purpose of the study is to provide student-level predictive analytics. Each student's journey through JCPS is highly specific to that student and unlikely to generalize into broad student groupings. Inclusion of student-specific data points with pertinent information (such as academic performance in specific courses, attendance, and behavior) will be a key component of any predictive model we are able to create. While EdjAnalytics will receive data on individual students, the data will be anonymized such that Edj staff cannot identify the true identity of the students.

Exhibit B

**RESEARCH ORGANIZATION'S EMPLOYEE OR
CONTRACTOR NONDISCLOSURE STATEMENT**

Include the completed Nondisclosure Statements or confidentiality agreement with your proposed DATA SHARING AGREEMENT.

Research Organization: EdjAnalytics, LLC

Research Organization's employee or contractor name: Brandon Debes

Title: Database Administrator

Address: 732 East Market Street, Louisville, KY 40202

Phone: 502-287-8257

I understand that the performance of my duties as an employee or contractor of the Research Organization involve a need to access and review confidential information (information designated as confidential by FERPA, NSLA, CNA, KRS 61.931(6), or other federal or state law); and, that I am required to maintain the confidentiality of this information and prevent any redisclosure prohibited under the law as stated below. By signing this document, I agree to the following:

- I will not permit access to confidential information to persons not authorized by the RESEARCH ORGANIZATION and its contractor.
- I will maintain the confidentiality of the data or information.
- I will not access data of persons related or known to me for personal reasons.
- I will not reveal any individually identifiable information furnished, acquired, retrieved, or assembled by me or others for any purpose other than statistical purposes specified in the RESEARCH ORGANIZATION survey, project, or proposed research.
- I will report, immediately and within twenty-four (24) hours, any known reasonably believed instances of missing data, data that has been inappropriately shared, or data taken off site
 - to my immediate supervisor, Associate Commissioner, and
 - to the Division of Human Resources if I am a RESEARCH ORGANIZATION employee or
 - to the RESEARCH ORGANIZATION Office for whom I perform work under the contract if I am a RESEARCH ORGANIZATION contractor or an employee of a RESEARCH ORGANIZATION contractor
- I understand that procedures must be in place for monitoring and protecting confidential information.
- I understand and acknowledge that FERPA-protected information obtained under provisions of Family Educational Rights and Privacy Act of 1974 (FERPA) as a RESEARCH ORGANIZATION contractor's employee or contractor of RESEARCH ORGANIZATION is confidential information.
- I understand that FERPA protects information in students' education records that are maintained by an educational agency or institution or by a party acting for the agency or institution, and includes, but is not limited to the student's name, the name of the student's parent or other family members, the address of the student or student's family, a personal identifier, such as the student's social security number, student number, or biometric record, other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name, and other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.
- I understand that any unauthorized disclosure of confidential information is illegal as provided in FERPA and in the implementing of federal regulations found in 34 CFR, Part 99. The penalty for unlawful disclosure is a fine of not more than \$250,000 (under 18 U.S.C. 3571) or imprisonment for not more than five years (under 18 U.S.C. 3559), or both.
- I understand and acknowledge that children's free and reduced price meal and free milk eligibility information or information from the family's application for eligibility, obtained under provisions of the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq)(NSLA) or Child

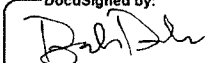
Nutrition Act of 1966 (42 U.S.C. 1771 et seq.)(CNA) and the regulations implementing these Acts, is confidential information.

- I understand that any unauthorized disclosure of confidential free and reduced price lunch information or information from an application for this benefit is illegal as provided in the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq.)(NSLA) or Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.)(CNA) and the regulations implementing these Acts, specifically 7 C.F.R. 245.6. The penalty for unlawful disclosure is a fine of not more than \$1,000.00 (under 7 C.F.R. 245.6) or imprisonment for up to one year (under 7 C.F.R. 245.6), or both.
- I understand that KRS 61.931 also defines "personal information" to include an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:
 - a) An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;
 - b) A Social Security number;
 - c) A taxpayer identification number that incorporates a Social Security number;
 - d) A driver's license number, state identification card number, or other individual identification number issued by any agency;
 - e) A passport number or other identification number issued by the United States government; or
 - f) Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g.
- I understand that other federal and state privacy laws protect confidential data not otherwise detailed above and I acknowledge my duty to maintain confidentiality of that data as well.
- I understand that any personal characteristics that could make the person's identity traceable, including membership in a group such as ethnicity or program area, are protected.

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

Research Organization employee or contractor signature:

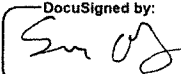
Date:

DocuSigned by:

 2071F0029F0641A

3/12/2020

Research Organization authorized agent signature:

Date:

DocuSigned by:

 BE11G54F08EA403...

3/12/2020

Research Organization authorized agent name (typed): Sean O'Leary

Research Organization: EdjAnalytics, LLC

Research Organization's employee or contractor name: Dennis Gomer

Title: Data Scientist, Director of IT

Address: 732 East Market Street, Louisville, KY 40202

Phone: 502-225-3016

I understand that the performance of my duties as an employee or contractor of the Research Organization involve a need to access and review confidential information (information designated as confidential by FERPA, NSLA, CNA, KRS 61.931(6), or other federal or state law); and, that I am required to maintain the confidentiality of this information and prevent any redisclosure prohibited under the law as stated below. By signing this document, I agree to the following:

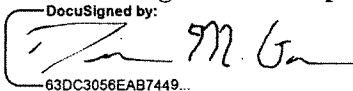
- I will not permit access to confidential information to persons not authorized by the RESEARCH ORGANIZATION and its contractor.
- I will maintain the confidentiality of the data or information.
- I will not access data of persons related or known to me for personal reasons.
- I will not reveal any individually identifiable information furnished, acquired, retrieved, or assembled by me or others for any purpose other than statistical purposes specified in the RESEARCH ORGANIZATION survey, project, or proposed research.
- I will report, immediately and within twenty-four (24) hours, any known reasonably believed instances of missing data, data that has been inappropriately shared, or data taken off site
 - to my immediate supervisor, Associate Commissioner, and
 - to the Division of Human Resources if I am a RESEARCH ORGANIZATION employee or
 - to the RESEARCH ORGANIZATION Office for whom I perform work under the contract if I am a RESEARCH ORGANIZATION contractor or an employee of a RESEARCH ORGANIZATION contractor
- I understand that procedures must be in place for monitoring and protecting confidential information.
- I understand and acknowledge that FERPA-protected information obtained under provisions of Family Educational Rights and Privacy Act of 1974 (FERPA) as a RESEARCH ORGANIZATION contractor's employee or contractor of RESEARCH ORGANIZATION is confidential information.
- I understand that FERPA protects information in students' education records that are maintained by an educational agency or institution or by a party acting for the agency or institution, and includes, but is not limited to the student's name, the name of the student's parent or other family members, the address of the student or student's family, a personal identifier, such as the student's social security number, student number, or biometric record, other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name, and other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.
- I understand that any unauthorized disclosure of confidential information is illegal as provided in FERPA and in the implementing of federal regulations found in 34 CFR, Part 99. The penalty for unlawful disclosure is a fine of not more than \$250,000 (under 18 U.S.C. 3571) or imprisonment for not more than five years (under 18 U.S.C. 3559), or both.
- I understand and acknowledge that children's free and reduced price meal and free milk eligibility information or information from the family's application for eligibility, obtained under provisions of the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq)(NSLA) or Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.)(CNA) and the regulations implementing these Acts, is confidential information.
- I understand that any unauthorized disclosure of confidential free and reduced price lunch information or information from an application for this benefit is illegal as provided in the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq)(NSLA) or Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.)(CNA) and the regulations implementing these Acts, specifically 7

C.F.R 245.6. The penalty for unlawful disclosure is a fine of not more than \$1,000.00 (under 7 C.F.R. 245.6) or imprisonment for up to one year (under 7 C.F.R. 245.6), or both.

- I understand that KRS 61.931 also defines "personal information" to include an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:
 - f) An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;
 - g) A Social Security number;
 - h) A taxpayer identification number that incorporates a Social Security number;
 - i) A driver's license number, state identification card number, or other individual identification number issued by any agency;
 - j) A passport number or other identification number issued by the United States government; or
 - f) Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g.
- I understand that other federal and state privacy laws protect confidential data not otherwise detailed above and I acknowledge my duty to maintain confidentiality of that data as well.
- I understand that any personal characteristics that could make the person's identity traceable, including membership in a group such as ethnicity or program area, are protected.

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

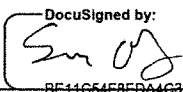
Research Organization employee or contractor signature:

DocuSigned by:

63DC3056EAB7449...

Date:

3/12/2020

Research Organization authorized agent signature:

DocuSigned by:

BE14C64F8EDA4G3...

Date:

3/12/2020

Research Organization authorized agent name (typed): Sean O'Leary

Research Organization: EdjAnalytics, LLC

Research Organization's employee or contractor name: Scott Brown

Title: Data Scientist

Address: 732 East Market Street, Louisville, KY 40202

Phone: 815-353-3041

I understand that the performance of my duties as an employee or contractor of the Research Organization involve a need to access and review confidential information (information designated as confidential by FERPA, NSLA, CNA, KRS 61.931(6), or other federal or state law); and, that I am required to maintain the confidentiality of this information and prevent any redisclosure prohibited under the law as stated below. By signing this document, I agree to the following:

- I will not permit access to confidential information to persons not authorized by the RESEARCH ORGANIZATION and its contractor.
- I will maintain the confidentiality of the data or information.
- I will not access data of persons related or known to me for personal reasons.
- I will not reveal any individually identifiable information furnished, acquired, retrieved, or assembled by me or others for any purpose other than statistical purposes specified in the RESEARCH ORGANIZATION survey, project, or proposed research.
- I will report, immediately and within twenty-four (24) hours, any known reasonably believed instances of missing data, data that has been inappropriately shared, or data taken off site
 - to my immediate supervisor, Associate Commissioner, and
 - to the Division of Human Resources if I am a RESEARCH ORGANIZATION employee or
 - to the RESEARCH ORGANIZATION Office for whom I perform work under the contract if I am a RESEARCH ORGANIZATION contractor or an employee of a RESEARCH ORGANIZATION contractor
- I understand that procedures must be in place for monitoring and protecting confidential information.
- I understand and acknowledge that FERPA-protected information obtained under provisions of Family Educational Rights and Privacy Act of 1974 (FERPA) as a RESEARCH ORGANIZATION contractor's employee or contractor of RESEARCH ORGANIZATION is confidential information.
- I understand that FERPA protects information in students' education records that are maintained by an educational agency or institution or by a party acting for the agency or institution, and includes, but is not limited to the student's name, the name of the student's parent or other family members, the address of the student or student's family, a personal identifier, such as the student's social security number, student number, or biometric record, other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name, and other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.
- I understand that any unauthorized disclosure of confidential information is illegal as provided in FERPA and in the implementing of federal regulations found in 34 CFR, Part 99. The penalty for unlawful disclosure is a fine of not more than \$250,000 (under 18 U.S.C. 3571) or imprisonment for not more than five years (under 18 U.S.C. 3559), or both.
- I understand and acknowledge that children's free and reduced price meal and free milk eligibility information or information from the family's application for eligibility, obtained under provisions of the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq)(NSLA) or Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.)(CNA) and the regulations implementing these Acts, is confidential information.
- I understand that any unauthorized disclosure of confidential free and reduced price lunch information or information from an application for this benefit is illegal as provided in the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq)(NSLA) or Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.)(CNA) and the regulations implementing these Acts, specifically 7


C.F.R. 245.6. The penalty for unlawful disclosure is a fine of not more than \$1,000.00 (under 7 C.F.R. 245.6) or imprisonment for up to one year (under 7 C.F.R. 245.6), or both.

- I understand that KRS 61.931 also defines "personal information" to include an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:
 - k) An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;
 - l) A Social Security number;
 - m) A taxpayer identification number that incorporates a Social Security number;
 - n) A driver's license number, state identification card number, or other individual identification number issued by any agency;
 - o) A passport number or other identification number issued by the United States government; or
 - f) Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g.
- I understand that other federal and state privacy laws protect confidential data not otherwise detailed above and I acknowledge my duty to maintain confidentiality of that data as well.
- I understand that any personal characteristics that could make the person's identity traceable, including membership in a group such as ethnicity or program area, are protected.

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

Research Organization employee or contractor signature:

Date:

DocuSigned by:

A5C8F4A3B5674D8...

3/12/2020

Research Organization authorized agent signature:

Date:

DocuSigned by:

BE11C54F8EDA4C3...

3/12/2020

Research Organization authorized agent name (typed): Sean O'Leary

Research Organization: EdjAnalytics, LLC

Research Organization's employee or contractor name: Michael Rayome

Title: Product Manager

Address: 732 East Market Street, Louisville, KY 40202

Phone: 502-208-4088

I understand that the performance of my duties as an employee or contractor of the Research Organization involve a need to access and review confidential information (information designated as confidential by FERPA, NSLA, CNA, KRS 61.931(6), or other federal or state law); and, that I am required to maintain the confidentiality of this information and prevent any redisclosure prohibited under the law as stated below. By signing this document, I agree to the following:

- I will not permit access to confidential information to persons not authorized by the RESEARCH ORGANIZATION and its contractor.
- I will maintain the confidentiality of the data or information.
- I will not access data of persons related or known to me for personal reasons.
- I will not reveal any individually identifiable information furnished, acquired, retrieved, or assembled by me or others for any purpose other than statistical purposes specified in the RESEARCH ORGANIZATION survey, project, or proposed research.
- I will report, immediately and within twenty-four (24) hours, any known reasonably believed instances of missing data, data that has been inappropriately shared, or data taken off site
 - to my immediate supervisor, Associate Commissioner, and
 - to the Division of Human Resources if I am a RESEARCH ORGANIZATION employee or
 - to the RESEARCH ORGANIZATION Office for whom I perform work under the contract if I am a RESEARCH ORGANIZATION contractor or an employee of a RESEARCH ORGANIZATION contractor
- I understand that procedures must be in place for monitoring and protecting confidential information.
- I understand and acknowledge that FERPA-protected information obtained under provisions of Family Educational Rights and Privacy Act of 1974 (FERPA) as a RESEARCH ORGANIZATION contractor's employee or contractor of RESEARCH ORGANIZATION is confidential information.
- I understand that FERPA protects information in students' education records that are maintained by an educational agency or institution or by a party acting for the agency or institution, and includes, but is not limited to the student's name, the name of the student's parent or other family members, the address of the student or student's family, a personal identifier, such as the student's social security number, student number, or biometric record, other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name, and other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.
- I understand that any unauthorized disclosure of confidential information is illegal as provided in FERPA and in the implementing of federal regulations found in 34 CFR, Part 99. The penalty for unlawful disclosure is a fine of not more than \$250,000 (under 18 U.S.C. 3571) or imprisonment for not more than five years (under 18 U.S.C. 3559), or both.
- I understand and acknowledge that children's free and reduced price meal and free milk eligibility information or information from the family's application for eligibility, obtained under provisions of the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq)(NSLA) or Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.)(CNA) and the regulations implementing these Acts, is confidential information.
- I understand that any unauthorized disclosure of confidential free and reduced price lunch information or information from an application for this benefit is illegal as provided in the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq)(NSLA) or Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.)(CNA) and the regulations implementing these Acts, specifically 7


C.F.R 245.6. The penalty for unlawful disclosure is a fine of not more than \$1,000.00 (under 7 C.F.R. 245.6) or imprisonment for up to one year (under 7 C.F.R. 245.6), or both.

- I understand that KRS 61.931 also defines "personal information" to include an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:
 - p) An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;
 - q) A Social Security number;
 - r) A taxpayer identification number that incorporates a Social Security number;
 - s) A driver's license number, state identification card number, or other individual identification number issued by any agency;
 - t) A passport number or other identification number issued by the United States government; or
 - f) Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g.
- I understand that other federal and state privacy laws protect confidential data not otherwise detailed above and I acknowledge my duty to maintain confidentiality of that data as well.
- I understand that any personal characteristics that could make the person's identity traceable, including membership in a group such as ethnicity or program area, are protected.

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

Research Organization employee or contractor signature:

Date:

DocuSigned by:

 3171EE388B70490...

3/12/2020

Research Organization authorized agent signature:

Date:

DocuSigned by:

 BE41C64F8EDA4C3...

3/12/2020

Research Organization authorized agent name (typed): Sean O'Leary

Exhibit C

Please describe the measures you take to ensure the protection of data released to you. If you have a policy, please attach or copy/paste here as Exhibit C and include information on the requested delivery method.

EdjAnalytics Data Protection Policy for JCPS

All electronic information from the Data Provider will be stored as received in a TrueCrypt encrypted disk image container as well as stored in a relational format in an encrypted PostgreSQL database. Any data transmitted to the encrypted database will be sent over SSL to ensure security in-motion as well as at rest.

Each data custodian designated in Exhibit D will be supplied with unique credentials to access the encrypted database, authorized only to the data each needs to perform his or her job function. All custodian activity on the database will be logged. Custodians will be given a copy of the data sharing agreement as well as instructions for appropriate data use, and each will sign the confidentiality agreement in Exhibit B. Only the Primary Data Custodian named in Exhibit A will have access to the TrueCrypt container(s) where original files are stored.

All devices used to access the encrypted data (via either source) will be Research Organization owned laptop computers, equipped with standard firewall and anti-virus software. Custodians will be instructed not to keep unencrypted copies on secure data locally outside of working sessions.

EdjAnalytics Client Data Security Policy

For any project which involves Edj taking receipt of sensitive client data, the following security policies will be applied:

User Access Management

Management and Access Control

Only the employee's supervisor or manager can grant access to EdjAnalytics sensitive client data information systems.

Access to the information system or application may be revoked or suspended, consistent with EdjAnalytics policies and practices, if there is evidence that an individual is misusing information or resources. Any individual whose access is revoked or suspended may be subject to disciplinary action or other appropriate corrective measures.

Minimum Necessary Access

EdjAnalytics shall ensure that only employees who require access to sensitive client data are granted access. Each supervisor or manager is responsible for ensuring that the access to sensitive client data granted to each of his or her subordinates is the minimum necessary access required for each subordinate's job role and responsibilities. If the user no longer requires access, it is the supervisor or manager's responsibility to complete the necessary process to terminate access.

Granting Access to Sensitive Client Data

Screen Employees Prior to Access

The manager or supervisor shall ensure that information access is granted only after first verifying that the access of an employee to sensitive client data is appropriate.

Sign Security Acknowledgement

Prior to being issued a User ID or log on account to access any sensitive client data, each employee shall sign EdjAnalytics's Confidentiality Agreement or an Acknowledgement of Information Security Responsibility before access is granted to the network or any application that contains sensitive client data, and thereafter shall comply with all EdjAnalytics's security policies and procedures.

Security Awareness Prior to Getting Access

Before access is granted in any of the various systems or applications that contain sensitive client data, employees shall be trained to a minimum standard including:

1. Proper uses and disclosures of the sensitive client data stored in systems or application(s)
2. How to properly log on and log off the systems or application(s)
3. Protocols for correcting user errors
4. Instructions on contacting a designated person or help desk when sensitive client data may have been altered or destroyed in error
5. Reporting a potential or actual security breach

Management Approval

1. User IDs or log on accounts can only be assigned with management approval.
2. Managers are responsible for requesting the appropriate level of computer access for staff to perform their job function.
3. All requests regarding User IDs or computer system access for employees are to be communicated to the appropriate individuals by email, for tracking purposes for EdjAnalytics. All requests shall be made in writing (which may be in an electronic format).
4. System administrators are required to process only those requests that have been authorized by managers.
5. Request is to be retained by the system administrator for a minimum of 1 year.

Termination of Access

The department manager or his/her designated representative is responsible for terminating an employee's access to sensitive client data in these circumstances:

1. If management has evidence or reason to believe that the individual is using information systems or resources in a manner inconsistent with EdjAnalytics's policies.
2. If the employee or management has evidence or reason to believe the user's password has been compromised.
3. If the employee resigns, is terminated, is suspended, retires, or is away on unapproved leave.
4. If the employee's job description changes and system access is no longer justified by the new job description.

If the employee is on an approved leave of absence and the user's system access will not be required for more than three weeks, management shall suspend the user's account until the employee returns from their leave of absence.

Modifications to the Employee's Access

If an employee transfers to another project or changes role(s) within the same project within EdjAnalytics:

1. The employee's new supervisor or manager is responsible for evaluating the member's current access and for requesting new access to sensitive client data commensurate with the employee's new role and responsibilities.

If an employee transfers to another program or department outside of EdjAnalytics:

1. The employee's access to sensitive client data within his or her current unit shall be terminated as of the date of transfer.
2. The employee's new supervisor or manager is responsible for requesting access to sensitive client data commensurate with the employee's new role and responsibilities.

Ongoing Compliance for Access

In order to ensure that employees only have access to sensitive client data when it is required for their job function, the following actions shall be implemented by EdjAnalytics:

1. Every new User ID or log on account that has not been used after 30 consecutive calendar days since creation shall be investigated to determine if the employee still requires access to the sensitive client data.
2. At least every six months, IT teams are required to send supervisors/managers (or appropriate designees):
 - a. A list of all employees for all applications.
 - b. A list of employees and their access rights for all shared folders that contain sensitive client data, and
 - c. A list of all Virtual Private Network (VPN) employees.
3. The supervisors/managers shall then notify their IT teams of any employees that no longer require access.

Authentication & Password Management

Information systems used to access sensitive client data shall uniquely identify and authenticate employees.

Authentication – Verification

Industry standard protocols will be used on all routers and switches used in the Wide Area Network (WAN) and the local area networks (LANs). Authentication types can include:

1. Unique user ID and passwords
2. Biometric identification system
3. Telephone callback
4. Token system that uses a physical device for user identification
5. Two forms of authentication for wireless remote access
6. Information systems used to access sensitive client data shall identify and authenticate connections to specific devices involved in system communications (digital certificate, for example)

The password file on the authenticating server shall be adequately protected and not stored unencrypted.

Unique User ID and Password Management

1. All EdjAnalytics employees are assigned a unique user ID to access the network. All employees are responsible for creating and maintaining the confidentiality of the password associated with their unique user ID. Managers/supervisors are required to ensure that their staff understands the user responsibilities for securely managing confidential passwords.
2. Upon receipt of a user ID, the person assigned to said ID is required to change the password provided by the administrator to a password that only he or she (the user) knows. Effective passwords shall be created in order to secure access to sensitive client data.
3. Employees who suspect that their password has become known by another person shall change their password immediately. No user shall give his or her password to another person.
4. Employees are required to change their network user ID passwords every six months; when the technology is capable. Each application access password shall be changed every six months. Where technology is capable, network and application systems shall be configured to enforce automatic expiration of passwords every six months.
5. All privileged system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) shall be changed at least each fiscal quarter. All passwords are to be treated as sensitive, confidential EdjAnalytics information.

3.3 User ID & Password Guidelines

Where possible, implement unique user IDs that are different from the e-mail address; EdjAnalytics is encouraged not to use standard naming conventions for user IDs and should avoid using the same email user name as the system user ID.

1. Password length:
 - a. 8-character passwords are the absolute minimum;
 - b. 10-12 characters or longer is recommended; and
 - c. Passwords up to 64 characters should be allowed.
2. Requiring mixed case, numbers, or special characters is recommended
3. Requiring users to periodically change their passwords is recommended:
 - a. Every 6 months or a year preferably.
 - b. Passwords are required to change if there is a suspicion that a password has been compromised.
4. Password selection software should not allow "obvious" passwords:
 - a. Common words, words related to the user, repeated letters, numeric sequences, etc. (e.g, "password123", "johnsmith", or "abcabcabc")
5. Login software should include features to prevent brute force attacks, such as:
 - a. Delays between login attempts; and
 - b. Lock account after a number of failed attempts.
6. Password protection requirements for users:
 - a. Never reveal a password over the phone to anyone;
 - b. Never reveal a password in an email message;
 - c. Never reveal a password to your supervisor;
 - d. Never talk about a password in front of others;
 - e. Never hint at the format of a password (e.g., "my family name");
 - f. Never reveal a password on questionnaires or security forms;
 - g. Never share a password with family members;
 - h. Never reveal a password to co-workers;
 - i. Never write down your password; instead, memorize it;
 - j. Never keep a list of user IDs and passwords in your office; and
 - k. Never misrepresent yourself by using another person's user ID and password.

- I. Use supplied password manager software where possible

Workstation Access Controls

Workstation Use: Security

1. EdjAnalytics members shall ensure that observable confidential information is adequately shielded from unauthorized disclosure and unauthorized access on computer screens. Each EdjAnalytics workplace shall make every effort to ensure that confidential information on computer screens is not visible to unauthorized persons.
2. Employees who work in other facilities that are not part of EdjAnalytics shall be aware of their surroundings to ensure no one can incidentally view sensitive client data and no sensitive client data is left unattended.
3. Employees who work from home or other non-office sites shall take the necessary steps to protect sensitive client data from other persons who may have access to their home or other non-office site. This includes security for all forms of portable sensitive client data such as locking up CD ROM Disks, floppy disks, USB drives, PDAs, and laptops. Because EdjAnalytics provides laptops to each employee, personal computers should not be used to access sensitive client data.
4. User session-lock shall be implemented when the computer is left idle. It shall be automatic after a specific time based on location and function. The session shall be locked to disable access to the PC until the user enters their unique password with login information.
5. When technology is capable, while accessing sensitive client data outside the EdjAnalytics Wide Area Network (for example: extranet, VPN) automatic log off shall occur after a maximum of 60 minutes of inactivity. Automatic log off is a system-enabled enforcement of session termination after a period of inactivity and blocks further access until the employee reestablishes the connection using the identification and authentication process.

Device and Media Controls

Device and Media Controls/Accountability

1. EdjAnalytics shall protect all hardware and electronic media that contains sensitive client data. This includes personal computers, PDAs, laptops, storage systems, backup tapes, CD ROM disks, and removable disks.
2. Every area of EdjAnalytics is responsible for developing procedures that govern the receipt and removal of hardware and electronic media that contain(s) sensitive client data into and out of a facility. Procedures shall include maintaining a record of movements of hardware and electronic media and any persons responsible.

Portable Media Use - Security

1. In addition to protecting EdjAnalytics's workstations and facilities, employees shall protect sensitive client data when working from all other locations. This includes locations such as home, other offices, or when working in the field.
2. In order to limit the amount of portable sensitive client data, employees **shall not** save any sensitive client data on floppy disks, CD ROM Disks and other portable items.
3. Methods for protecting portable media with sensitive client data include:
 - a. All employees shall receive permission from their supervisor before removing sensitive client data from their facility. Approvals shall include the type of permission and the time period for authorization. The time period shall be a maximum of one year.
 - b. Employees who work in the field shall not leave sensitive client data unlocked or visible in their vehicles. They will also not leave any sensitive client data in client facilities/homes.
 - c. If sensitive client data is lost, employees are responsible for promptly contacting their supervisor within one business day upon awareness that sensitive client data has been lost.

Disposal

1. Before electronic media that contains sensitive client data can be disposed, the following actions shall be taken on computers used in the workplace, at home, or at remote sites:
 - a. Hard drives shall be either wiped clean or destroyed. Hard drive cleaning shall meet the Department of Defense (DOD) standards, which states, "*The method of destruction shall preclude recognition or*

reconstruction of the classified information or material.” In addition, the hard drive shall be tested to ensure the information cannot be retrieved.

- b. Backup tapes shall be destroyed or returned to the owner and their return documented. Destruction shall include a method to ensure there is no ability to reconstruct the data.
- c. Other media, such as memory sticks, USB flash drives or micro drives, CD-ROMs and floppy disks, shall be physically destroyed (broken into pieces) before disposing of the item.

Media Reuse

1. All sensitive client data shall be removed from hard drives when the equipment is transferred to a worker who does not require access to the sensitive client data, or when the equipment is transferred to a new worker with different sensitive client data access needs. Hard drives shall be wiped clean before transfer.
2. Cleaning shall meet the Department of Defense (DOD) standards, which states, *“The method of destruction shall preclude recognition or reconstruction of the classified information or material.”* In addition, the hard drive shall be tested to ensure the information cannot be retrieved.

Sending a Computer Server Hard Drive to Repair

When the technology is capable, an exact copy of the sensitive client data shall be created and the sensitive client data removed from the server hard drive before sending the device out for repair.

Moving Computer Server Equipment with sensitive client data

Before moving server equipment that contains sensitive client data, a retrievable exact copy needs to be created.

Device and Media Acquisition

EdjAnalytics shall include security requirements and/or security specifications in information system acquisition contracts based on an assessment of risk (applications, servers, copiers, etc.).

Audit Controls

Log-in Monitoring

1. EdjAnalytics has the right to monitor system access and activity of all employees.
2. To ensure that access to servers, workstations, and other computer systems containing sensitive client data is appropriately secured; the following login monitoring measures shall be implemented:
 - a. A mechanism to log and document four or more failed log-in attempts in a row shall be implemented on each network system containing sensitive client data when the technology is capable.
 - b. Login activity reports and logs shall be reviewed biweekly at a minimum to identify any patterns of suspicious activity.
 - c. All failed login attempts of a suspicious nature, such as continuous attempts, shall be reported immediately to the Security Officer or the designee for EdjAnalytics.
 - d. To the extent that technology allows, any user ID that has more than four-repeated failed login attempts in a row shall be disabled for a minimum of 30 minutes.

Information System Activity Review – Audit Controls

To ensure that activity for all computer systems accessing sensitive client data is appropriately monitored and reviewed, these requirements shall be met:

1. Where technology allows, the audit record shall capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
2. Each fiscal quarter, at a minimum, every application and system administrator or designee shall review audit logs, activity reports, or other mechanisms to document and manage system activity.
3. Indications of improper use shall be reported to management for investigation and follow up.
4. Audit logs of access to networks and applications with sensitive client data shall be archived.
5. Audit information and audit tools shall be protected from unauthorized access, modification, and deletion.

Transmission Security

EdjAnalytics shall employ tools and techniques to monitor events, detect attacks, and provide identification of unauthorized use of the systems that contain sensitive client data.

Reporting

1. All security incidents, threats, or violations that affect or may affect the confidentiality, integrity or availability of electronic protected health information (sensitive client data) shall be reported and responded to promptly.
2. Incidents that shall be reported include, but are not limited to:
 - a. Virus, worm, or other malicious code attacks;
 - b. Network or system intrusions;
 - c. Persistent intrusion attempts from a particular entity;
 - d. Unauthorized access to sensitive client data, a sensitive-client-data-based system, or a sensitive-client-data-based network;
 - e. sensitive client data loss due to disaster, failure, error, theft;
 - f. Loss of any electronic media that contains sensitive client data;
 - g. Loss of the integrity of sensitive client data; and
 - h. Unauthorized person found in EdjAnalytics's facility.
3. EdjAnalytics's Compliance Officers shall be notified immediately of any suspected or real security incident. If it is unclear as to whether a situation is a security incident, the Compliance Officers shall be contacted to evaluate the situation.

Response and Resolution

The Compliance Officers shall track the incident. The Compliance Officers shall determine if a report of the incident shall be forwarded to the affected client(s). Compliance Officers are the only employees that can resolve an incident. The Compliance Officers shall evaluate the report to determine if an investigation of the incident is necessary. The Compliance Officers shall determine if EdjAnalytics's Counsel, law enforcement, Human Resources, or EdjAnalytics's Communication and Media Office is to be contacted regarding the incident.

Logging

1. All security-related incidents and their outcomes shall be logged and documented by the Compliance Officers. The Compliance Officers shall document and log incidents and outcomes.
2. All incident(s) will be reviewed and investigated and if the breached client data has been compromised (unauthorized individuals have received and viewed the client data) the breach will be reported to the affected client(s). EdjAnalytics and its Compliance Officers will record all the incidents and retain these incident reports for six years.
3. EdjAnalytics shall train personnel in their incident response roles and responsibilities and provide refresher training as needed. EdjAnalytics shall test the incident response capability at least annually using tests and exercises to determine the effectiveness.

Transmission Security

Encryption:

Proven, standard algorithms shall be used as the basis for encryption technologies. The use of proprietary encryption algorithms is not allowed for any purpose unless authorized by the Security Officer.

Encryption Required:

1. No sensitive client data shall be sent outside EdjAnalytics domain unless it is encrypted. This includes all email and email attachments sent over a public internet connection.
2. When accessing a secure network an encryption communication method, such as a VPN, shall be used.

Encryption Optional:

1. When using a point-to-point communication protocol to transmit sensitive client data, no encryption is required.
2. Dial-up connections directly into secure networks are considered to be secure connections for sensitive client data and no encryption is required.

Sensitive Client Data Transmissions Using Wireless LANs and Devices within EdjAnalytics domain:

- A) The transmission of sensitive client data over a wireless network within EdjAnalytics's domain is permitted if both of the following conditions are met:
 1. The local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized; and
 2. The local wireless network is utilizing an encryption mechanism for all transmissions over the aforementioned wireless network and uses two types of authentication.

B) If transmitting sensitive client data over a wireless network that is not utilizing an authentication and encryption mechanism, the sensitive client data shall be encrypted before transmission.

Perimeter Security

1. Any external connection to EdjAnalytics Wide Area Network (WAN) shall come through the perimeter security's Firewall.
2. If determined safe by the Security Officer, outbound services shall be initiated for internal addresses to external addresses.
3. Inbound services shall be negotiated on a case-by-case basis with the Security Officer.
4. All employees connecting to the WAN shall sign EdjAnalytics IT Confidentiality Agreement before connectivity is established.

Firewall Controls to Transmit sensitive client data Into and Out of EdjAnalytics

1. Networks containing systems and applications with sensitive client data shall implement perimeter security and access control with a firewall.
2. Firewalls shall be configured to support the following minimum requirements:
 - A. Limit network access to only authorized employees and entities;
 - B. Limit network access to only legitimate or established connections (An established connection is return - traffic in response to an application request submitted from within the secure network.); and
 - C. Console and other management ports shall be appropriately secured or disabled.
3. The configuration of firewalls used to protect networks containing sensitive client data-based systems and applications shall be submitted to the Security Officer for review and approval.

Protection from Malicious Software

EdjAnalytics shall ensure all computers (owned, leased, and/or operated by EdjAnalytics) are installed with and maintain anti-virus software. All workstations shall be configured to activate and update anti-virus software automatically each time the computer is turned on or the user logs onto the network.

In the event that a virus, worm, or other malicious code has infected or been identified on a server or workstation, that equipment shall be disconnected from the network until it has been appropriately cleaned.

Monitoring and Effectiveness

Risk Assessment & Management

EdjAnalytics, along with the Security Officer, shall monitor the effectiveness of EdjAnalytics's ability to secure sensitive client data. In order to accomplish this, a risk assessment shall be conducted when:

1. New technology is implemented that either contains sensitive client data or is used to protect sensitive client data;
2. New facilities that maintain or house sensitive client data are designed;
3. Existing facilities that maintain or house sensitive client data are being remodeled or the design layout is being altered;
4. New programs, functions, or departments are added that affect the security of EdjAnalytics;
5. Security breaches are identified; and
6. Changes in the mode or manner of service delivery are made.

Security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level shall be documented and implemented.

Change Control

The primary goal of change management is to facilitate communications and coordinate all changes that may occur in the IT environment. These changes include, but are not limited to, the installation, update, or removal of network services and components, operating system upgrades, application or database servers and software.

Change Notification

1. For informational purposes, the Security Officer shall be notified of changes by email no less than 48 hours in advance.
2. Emergency Changes shall be communicated to the Security Officer as soon as is reasonable.

3. Any change that encounters difficulties that could adversely affect customers, patients, or clients shall be communicated to the Security Officer as soon as is reasonable.

Change Implementation

All non-emergency changes shall occur within the recognized downtime unless approved in advance by all affected parties or for inter-departmental changes as department procedures dictate.

Change Closure

The disposition of all changes shall be documented.

Evaluation

EdjAnalytics shall conduct an assessment of security controls at least annually to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome. Technical and non-technical evaluations are to be conducted periodically to identify any new risks or to determine the effectiveness of the Security Policies and Procedures. These evaluations include but are not limited to the following:

1. Random audit reviews of a facility's physical environment security;
2. Random audit reviews of workstation security;
3. Periodic, unannounced tests of the physical, technical, and administrative controls;
4. Assessment of changes in the environment or business process that may affect the Security Policies and Procedures;
5. Assessment when new federal, state or local laws and regulations are passed that may affect the Security Policies and Procedures;
6. Assessment of the effectiveness of the Security Policies and Procedures when security violations, breaches or other security incidents occur; and
7. Assessment of redundancy needed in the network or servers for sensitive client data availability.

Exhibit D

Please describe the methods Research Organization will use to irrevocably destroy, wipe or sanitize all personal or confidential data at the completion of the study. This includes all formats and media including but not limited to paper, electronic, magnetic as well as any internal hard drive of a printer or copier prior to its disposal, relocation or being sent to surplus. Please specify the planned date of destruction for each format and media that is applicable. If you have a policy that describes the methods you will use to destroy all confidential data, it can be attached as Exhibit D. Research Organization's Certificate of Destruction (Exhibit E) is required for certification that all forms of personal or confidential data have been irrevocably destroyed, wiped or sanitized.

EdjAnalytics Response

Upon the conclusion of the study, the single copy of the master TrueCrypt container holding the original data files will be deleted using secure deletion software (to "zero-out bytes" of the file). The EC2 instance will be securely destroyed using Amazon AWS's secure instance destruction tool. Data custodians should not at that time have any remaining traces of the data on their devices, but we will ensure this is the case by collecting the devices and examining their storage media. Any found information from the Data Provider will be securely deleted (zeroed-out). It is not anticipated for any hard copies of the data to be created, but in the event that they are, such copies will be destroyed by cross-cut shredding. The study is expected to conclude on June 30th, 2018 so it is anticipated that secure data destruction will take place within two business days of same.

In alphabetical order by last name, provide information for those persons designated as data custodians. This should include anyone with access to confidential data. A designated primary and secondary data custodian are required and a minimum of four is requested. A signed Confidentiality Agreement or Data Provider's Nondisclosure Statement labeled Exhibit B is required for each data custodian.

(Prior to designating additional data custodians who are not listed on Exhibit D at the time the DATA SHARING AGREEMENT is executed, Research Organization must submit a written request and DATA SHARING AGREEMENT amendment will be required.)

Primary Data Custodian

Last Name, First Name: Debes, Brandon
 Phone: 502-287-8257
 Email: BDebes@edjanalytics.com
 Employer: EdjAnalytics, LLC

Secondary Data Custodian

Last Name, First Name: Gomer, Dennis
 Phone: 502-225-3016
 Email: DGomer@edjanalytics.com
 Employer: EdjAnalytics, LLC

All Other Data Custodians

Last Name, First Name: Brown, Scott
 Phone: 813-353-3041
 Email: sbrown@edjanalytics.com
 Employer: EdjAnalytics, LLC

Last Name, First Name: Rayome, Michael
 Phone: 502-208-4088
 Email: rrayome@edjanalytics.com
 Employer: EdjAnalytics, LLC

Exhibit E**RESEARCH ORGANIZATION'S CERTIFICATE OF DATA DESTRUCTION**

The Research Organization shall irreversibly destroy all copies of all confidential and otherwise personally identifiable data regardless of format (e.g. paper, electronic) within forty-five (45) days after it is no longer needed to perform the studies described in this agreement, upon DATA PROVIDER's request or upon termination of this agreement, whichever occurs first unless agreed otherwise in writing. Using this form, the Research Organization shall provide written verification of the data destruction to the DATA PROVIDER within forty-five (45) days after the data is destroyed. Scan the signed Certificate of Data Destruction and return it to Dr. Dena Dossett, Chief, Accountability, Research, and Systems Improvement.

If the Research Organization uses a contractor for data destruction services, a certificate of destruction from the contractor is also required. Please submit the contractor's certificate of destruction with this signed Certificate of Data Destruction.

In accord with the provisions of the DATA SHARING AGREEMENT between the Data Provider and the ("Research Organization" or "Contractor"), the confidential and otherwise personally identifiable data were destroyed as required in Section N according to the methods described in Exhibit D of the DATA SHARING AGREEMENT.

Date submitted:

Scheduled date of destruction (per DATA SHARING AGREEMENT):

Actual destruction date:

Media type	Method of Destruction	Comments

I hereby certify that all confidential and otherwise personally identifiable data described above have been destroyed in the manner indicated.

Research Organization Authorized Agent Signature:

Date:

DocuSigned by:

 BE41664F8ED4A08...

3/12/2020

Agent's Name: Sean O'Leary

Agent's Title: CEO and Co-Founder