APPENDIX A – USBE Application for External Research Data Sharing Agreement

Contact Information:
Utah State Board of Education
Dr. Whitney Phillips
Chief Privacy Officer
Whitney.phillips@schools.utah.gov
801-538-7523

I. External Researcher Information

A. Name of primary researcher(s), Ellie Young & Leanne Hawken
B. title, Associate Professor, Professor
C. organization, Brigham Young University & University of Utah,
D. brief description of the organization, Private and state universities
E. address, (For Ellie Young, who will be the corresponding author for this request)
340-L MCKB, Brigham Young University, Provo, UT 84602
F. phone, 801 422-1593
G. e-mail, ellie_young@byu.edu (USBE until June 23: ellie.young@schools.utah.gov)
H. website, http://education.byu.edu/directory/view/ellie-young
I. USBE Sponsor: Glenna Gallo, State Director of Special Education, 801 538-7898
glenna.gallo@school.utah.gov
J. Attach Curriculum vitae for external researcher(s).

II. Purpose

This project includes writing a research articles that summarizes the required annual reports of the Utah Multi-Tiered Systems of Supports (UMTSS) project, which is funded by the federal Office of Special Education Programs (OSEP).

Utah is viewed as a national leader in implementing multi-tiered systems of support (MTSS). At national conferences and in other settings Utah leaders are sought out to share their efforts to disseminate and implement MTSS in schools and school districts. The lessons we have learned have not yet been shared in the extant research literature. The article will provide the field with evidence-based strategies for state implementation teams to use when supporting local school districts who are implementing MTSS.

1. Project Title: Lessons Learned from a State Implementation Team to Support LEA-Level Implementation of MTSS: A Descriptive Study

2. Potential benefits to USBE: Establish Utah as a leader in implementing MTSS and highlighting the good work that USBE has done to support the implementation of innovative practices targeted to improve student outcomes.

3. Potential Risks to USBE: The preponderance of the data show marked improvement in implementation over time. However, the implementation is not yet perfect and some aspects of the implementation can be improved. The manuscript will highlight lessons learned and ideas for improved future implementation.

4. Will the requestor use this data for marketing purposes? No.

5. Will the requestor sell this data? No.

III. Roles

A. The Data Steward for this use case is Patsy Mulligan, although Ellie Young and Leanne Hawken have the data as part of the UMTSS reports for OSEP.

B. USBE's Data Quality manager is Aaron Brough.

C. Data may only be accessed, viewed, or used by the Researcher staff identified in this Appendix. Researcher may identify additional staff who require access to Data and provide that request to USBE in writing for review and consideration. Researcher staff with permission to view, access, or use Data include: Sara Moulton, Post Doctoral Employee, Brigham Young University. Devin Healey, Davis School District Employee and former UMTSS Project Director, Heidi Mucha, UMTSS Evaluator, and Cathy Callow-Heuser, USBE Education Specialist.

IV. Request

A. We are requesting to use the annual reports of the UMTSS project and the data in the correspondent Excel files that are used to complete the annual report. These annual reports were submitted to OSEP as part of a federally funded professional development grant. I am attaching a copy of the 2017 report to show the data that is already gathered and available. Only the data from these annual reports is being requested.

Any reporting of the data will not include identifying specific districts or schools. The LEA identity will be sufficiently masked so that no LEA can be identified.

1. Desired delivery date: June 10, 2017
2. Include level of data being requested
X State
X LEA
□ School
□ Teacher/Class
□ Student (De-identified)
□ Other

3. Data Category

The data we are requesting does not fit into these categories. The data is included in the annual reports of the UMTSS project to OSEP. The reports are currently being stored in a shared google drive that only the UMTSS team can access.

□ Accountability (AYP, NCLB)
□ Adult Education
□ Assessment (CRT, NAEP, DWA, etc.)
□ Career & Technical Education
□ Class Size
□ Course Enrollment
□ Data on Schools (i.e. how many, location, type)
□ Educator/Staff
□ Electronic High School
□ English Language Learners
□ Enrollment
□ Federal Programs
□ Free & Reduced Price Lunch
□ Graduation/Dropout
□ Internal USOE Accounting Membership
□ PATI
□ Progress Scores
□ Race/Ethnicity
□ School Budget/Finance
□ Special Education
□ Youth In Care (YIC)

Additional Information:

V. Output

See the attached document titled Project Narrative Section A 2017.

The research article will be based on this data. Similar reports from previous years (2014-2016) will also be accessed.

Data Linkage

A.

The data will not be linked to any other sources of data. The data are currently being stored on a google drive that only UMTSS personnel can access. The data also has been reported to OSEP project officers and their reviewers, which is required by OSEP. Only the researchers will use the data. Once the manuscript is completed and submitted to a research journal, journal reviewers and editors will see the aggregated data as part of the research article. Names of LEAs will not be provided in the article/s but rather each LEA will be assigned a number

VI. Participating Agencies

A. The Utah State Board of Education (USBE) will be sharing data with the Ellie Young and Leanne Hawken, professors at Brigham Young University and the University of Utah respectively.

VII. Duration of Study

A. The study referenced in this Appendix will end on December 31, 2017.

VIII. Research Questions, Variables of Interest, and Analytic Approach

Question	Variables	Analysis
To what extent have the participating 10 LEAs implemented the core features of UMTSS as measured by the UMTSS practice profile? An LEA level practice profile was created by the UMTSS state implementation team.	Scores on the practice profile completed by LEAs.	Descriptive summaries of change in scores from 2013 to 2017. No identifiable information of any school or LEA will be reported.
To what extent have the 10 participating LEAs moved through the stages of implementation as adapted from the National Implementation Research Network?	The state coach and district leadership team determines the stage of implementation by reviewing the required activities for each stage.	Descriptive summaries of change in scores from 2013 to 2017. No identifiable information of any school or LEA will be reported.
To what extent have school building leadership teams (BLT) engaged in team-initiated problem solving practices with fidelity?	The project used the Team Initiated Problem Solving (TIPS) Fidelity Checklist, which can be found online at www.pbis.org.	A summary of the TIPS checklist scores. Data will be reported LEA and as summary data for the 10 LEAs involved in the UMTSS project. No identifiable information of any school or LEA will be reported.
To what extent did the school teams implement core features of MTSS with fidelity?	The project used fidelity measures based on the content area of focus for the LEA. For the LEAs focusing on behavior, the School-wide Evaluation Tool (SET) or the Tiered Fidelity Inventory (TFI) was used. For the LEAs focusing on	A summary of scores. No identifiable information of any school or LEA will be reported.

Question	Variables	Analysis
	literacy the Reading School-wide Evaluation Tool f(R-SET) was used.	
How much coaching time did LEAs receive from the state UMTSS coaches?	Data from coaching logs.	Summary of descriptive data (i.e., number of hours coaching per month). No identifiable information from any school or LEA will be reported.
How did LEA systems coaches self-evaluate their coaching within their LEA?	Data from the coaching self-assessment.	Summary descriptive data. No identifiable information from any school or LEA will be reported.
Did more LEAs have coaches participate in the annual coaching institute?	Participation in the annual coaching institute.	Summary descriptive data. No identifiable information from any school or LEA will be reported.

IX. Regulations that Apply

A. FERPA (34 CFR Part 99, section 99.3)

B. The Student Data Protection Act, U.C.A §53A-1-1401 *et seq*. ("SDPA").

X. Signatures

To further the collection and analysis of Utah educational Data, USBE and Researcher agree to the cooperative sharing of Data between the Parties pursuant to the conditions set forth herein.

Signature: ______________________________ Date: _______________

Primary Researcher Title:________________________________

Organization:___________________________

External Research Data Sharing Agreement between the Utah State Board of Education (USBE) and Ellie Young and Leanne Hawken

This Research Data Sharing Agreement (Agreement) is entered into by and between the Utah State Board of Education (USBE), 250 East 500 South Salt Lake City, UT 84114 and Ellie Young and Leanne Hawken whose address is 340 MCKB, BYU, Provo, UT 84602 and Department of Special Education, University of Utah, 1721 Campus Center Drive, SAEC, Room #2287, Salt Lake City, Utah 84112 each individually a Party and together the Parties.

II. Definitions

A. "Aggregate Data" means data collected and reported at the group, cohort, or institutional level that is aggregated using protocols that are effective for preserving the anonymity of each individual included in the data.

B. “Data” includes Student Personally Identifiable Information and Educator Data.

C. “Data Breach” means unauthorized or unintentional use, exposure, disclosure, or loss of Data.

D. “Data Governance” means the oversight of data quality, data management, data policies, business process management, and risk management surrounding the handling of Data, and includes a set of processes that ensures that important Data assets are formally managed throughout the Party’s department, organization, or enterprise.

E. “Data Governance Manager” means the individual responsible for the implementation and oversight of the Party’s data management goals, standards, practices, processes, and policies.

F. “Data Owner” is the individual with responsibility and authority for an entrusted data resource. The data owner takes ownership of the operational, technical, and informational management of the PII.

G. “Data Steward” means the entity responsible for combining two data sets from different sources, and managing the resultant data set. If a USBE data system is being used, then USBE is the Data Steward. If another entity is doing the calculations or derivations, then that entity becomes the Data Steward.

H. "Destroy" means to remove Data from Researcher’s systems, paper files, records, databases, and any other media regardless of format, in accordance with the standard detailed in NIST Special Publication 800-88 Guidelines for Media Sanitization so that Data is permanently irretrievable in the Researcher’s normal course of business.

I. “Educator Data” includes, but is not limited to, the educator’s name; any unique identifier, including social security number; and other information that, alone or in combination, is linked or linkable to a specific educator.

J. “Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g” means the federal law that protects the privacy of students' personally identifiable information.

a. “Incident” means an accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources of the State pursuant to Student Data Protection Act, U.C.A §53A-1-1401 *et seq*. (“SDPA”).

Incidents include, but are not limited to (i) successful attempts to gain unauthorized access to a State system or Data regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a State system for the processing or storage of data; (iv) changes to State system hardware, firmware, or software characteristics without the State’s knowledge, instruction, or consent; or (v) a breach of this Agreement that results in the misuse or unauthorized disclosure of Data.

K. “Student Data Protection Act”, U.C.A §53A-1-1401 *et seq*. (“SDPA”) Utah state statute that became effective on May 10, 2016.

L. "Student Personally Identifiable Information (PII)" means information that is collected, maintained, generated, or inferred and that, alone or in combination, personally identifies an individual student or the student's parent or family. PII also includes other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

M. “Targeted Advertising” means selecting and sending advertisements to a student based on information obtained or inferred over time from the student’s online behavior, use of applications, or PII. Targeted Advertising does not include advertising to a student at an online location based on the student’s current visit to that location or in response to the student’s request for information or feedback and is without the collection and retention of a student’s online activities over time. Targeted Advertising also does not include adaptive learning, personalized learning, or customized education.

III. Purpose and Scope of Agreement

A. USBE is the state education agency responsible for the implementation of education laws adopted by the State of Utah. In fulfillment of law found in the Utah Revised Statutes, USBE is charged with collecting and securely maintaining data on students enrolled in the state’s Local Education Agencies (LEAs).

B. USBE and Researcher enter into this Research Data Sharing Agreement (Agreement) to share and exchange Data for the purposes of conducting studies for, or on behalf of, educational agencies or institutions to develop, validate, or administer predictive tests; administer student aid programs; or improve instruction.

C. This Agreement applies to all data sharing between Researcher and USBE. Specific data to be shared are outlined in attached appendices, along with the purpose of data sharing, data ownership and conditions and/or regulations governing the usage of the shared data, requirements for shared data retention/destruction, and Party processes for implementing these actions.

D. This Agreement shall expire in 12 months from the data of execution. Any Party desiring to extend the Agreement shall give at least 90 days advance notice by providing a notice of intent to renew to the other Party. Renewal shall only take place after review and possible update by both Parties. Renewals may only be in 12-month increments and the Agreement may not extend beyond a term of 5 years.

E. This Agreement shall be used exclusively for those uses permitted under the Family Education Rights and Privacy Act (FERPA), Utah's Student Data Transparency and Security Act, and any other pertinent federal or state statutes and regulations.

IV. General Provisions

A. Pursuant to Utah's Student Data Protection Act, USBE and LEAs cannot share student PII for the sole purpose of conducting external research.

B. USBE reserves all right, title, and interest, including all intellectual property and proprietary rights, in and to Data and all related content.

C. Researcher shall comply with the Family Education Rights and Privacy Act (FERPA), Utah's Student Data Protection Act, and any other pertinent federal or state statutes and regulations.

D. Researcher shall immediately forward to USBE's principal representative any request or demand from a third party for Data in the possession of Researcher.

E. Upon request of USBE or of the Utah State Board of Education, Researcher shall submit its data processing facilities for an audit of the measures referred to in this Agreement by USBE or by a USBE-approved delegate.

F. Researcher shall send USBE a written notice that includes a clear explanation of the proposed changes prior to making a material change to Researcher's privacy policies.

V. Use of Data

A. Researcher shall not use or share Data beyond the purposes set forth in the Appendices. Any request to use or share Data outside of this Agreement must be submitted in writing to USBE and USBE and Researcher will have to amend this Agreement or add additional Appendices that fully describe the new uses or sharing of Data.

B. In the event the Agreement requires Researcher to store, process or transfer Data, Researcher shall store, process, and transfer Data only in or to facilities located within the United States.

C. During the term of this Agreement, if USBE requests the destruction of data collected, generated or inferred as a result of this Agreement, Researcher shall Destroy the information within five calendar days after the date of the request unless:

D. If Researcher seeks to share or publically release Data, Researcher must de-identify or aggregate student-level data prior to releasing the data publically. The following requirements apply for Data to be considered Aggregate Data:

1. Data to be aggregated or de-identified shall include not only direct identifiers, such as names, student IDs, but also any other sensitive and non-sensitive information that, alone or combined with other information that is linked or linkable to a specific individual, would allow identification.

2. Researcher agrees to not report or publish Subject Data in any manner that discloses students' identities in accordance with the Family Educational Rights and Privacy Act (FERPA), 34 CFR 99-31 (a) (6), such as publishing performance data for subgroups of students with a count, also known as n-size, less than 10. Researcher agrees not to make any effort to discover the identity of a subject.

3. Simple removal of direct identifiers from the Data to be released shall not constitute adequate de-identification.

4. Researcher shall de-identify Data to remove cumulative re-identification risks.

5. Researcher shall remove all Data that in conjunction with previous data releases and other reasonably available information, including publicly available directory information and de-identified data releases from education records and other sources would allow for identification of a particular student.

6. Researcher shall have specific steps and methods used to de-identify or aggregate Data to protect the confidentiality of individuals. Researcher shall, at the request of USBE, provide USBE with a document that lists the steps and methods Researcher shall use to de-identify Data.

E. Prior to public dissemination/release, Researcher shall provide an electronic copy of each report or publication researcher produces using USBE data to the USBE's State Superintendent of Public Instruction at least 10 business days prior to the public release reports or documentation generated as a result of using. USBE will ensure that access to the report is permitted on a need-to-know basis only for this verification purpose and will protect the report from public dissemination or release.

F. USBE reserves the right to receive a final copy of the research report and post that report on USBE's public facing website.

G. Researcher understands that the USBE may publish annotated bibliographic information about the researcher's work but will not reproduce the report for distribution outside of the USBE without express written permission from the copyright holder.

VI. Disallowed Activities

A. Researcher shall not disclose Data to any third party.

B. Researcher may not use Data in a manner that is inconsistent with Researcher's privacy policy.

C. Researcher shall not sell Data, except that this prohibition does not apply to the purchase, merger, or other type of acquisition of Researcher, or any assets of Researcher, by another entity, so long as the successor entity continues to be subject to the provisions of this Agreement.

D. Researcher shall not use or share Data with any party for the purposes of Targeted Advertising to students.

E. Researcher shall not use Data to create a personal profile of a student other than for supporting the purposes authorized by USBE or with the consent of the student (provided that the student is over the age of 18) or the student's parent or legal guardian.

F. Researcher shall not publish reports with a cell size of less than 10 or that includes Data that has not been aggregated or de-identified as specified in this Agreement. Any Data that is not properly de-identified or aggregated and is publically released by Researcher will be considered an Incident.

G. Researcher shall not maintain or forward PII to or from any other facility or location outside of the Researcher's organization.

H. There shall be no disclosure of Data to government agencies outside of the state.

VII. Data Security

A. Researcher shall maintain a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of Data. At a minimum, the information security program shall include the requirements listed in this Section VI – Data Security.

B. Researcher shall provide physical and logical protection for all related hardware, software, applications, and data that meet or exceed industry standards and requirements as set forth in this Agreement. Researcher shall take full responsibility for the security of all Data in its possession, and shall hold USBE harmless for any damages or liabilities resulting from the unauthorized disclosure or loss thereof. Researcher shall provide for the security of Data, in a form acceptable to USBE, including, without limitation, non-disclosure, use of appropriate technology, security practices, computer access security, data access security, data storage encryption, data transmission encryption, security inspections, network firewalls, intrusion detection (host and network), data security logging and monitoring systems, and audits.

C. Researcher shall provide USBE or its designated representatives with access, subject to Researcher's reasonable access security requirements, for the purpose of inspecting and monitoring access and use of Data and evaluating physical and logical security control effectiveness.

D. Researcher shall perform, in a form reasonably acceptable to USBE, current background checks on all of its respective employees and agents identified as requiring access to Data in the Appendices. The background checks must include, but are not limited to the following areas: County, State, National and Federal Criminal Records and a Sex Offender Registry Search. A background check performed within thirty (30) calendar days prior to the date such employee or agent begins performance or obtains access to Data shall be deemed to be current.

E. Researcher shall have strong access controls, including role-based access to ensure that only authorized individuals have access to Data.

F. Workstations and other data processing devices must automatically lock when not in use, and must be manually locked when left unattended.

G. Researcher shall protect all Data with a complex password. Researcher shall ensure passwords are confidential and prohibit the sharing of passwords. Passwords must not be written down or stored in an unsecure location. Researcher shall periodically change passwords and shall ensure passwords are not reused. Researcher shall have password locks for laptops and mobile devices.

H. Researcher shall disable and/or immediately delete unused and terminated user accounts. Researcher shall periodically assess account inactivity for potential stale accounts.

I. Researcher shall not share Data on display screens, during demonstrations or presentations, or when sharing screen shots for troubleshooting or other purposes.

J. Researcher shall implement annual intrusion penetration/vulnerability testing.

K. Researcher shall encrypt Data at rest on central computing systems. Researcher shall also encrypt any backup, backup media, removable media, tape, or other copies. In addition, Researcher shall fully encrypt disks and storage for all laptops and mobile devices.

L. Researcher shall provide annual, mandatory security awareness and Data handling training for all of its employees handling Data pursuant to this Agreement.

M. Researcher shall install and maintain on computers accessing or processing Data appropriate endpoint security anti-virus and anti-malware software. Researcher shall ensure all Researcher's data processing systems, servers, laptops, PCs, and mobile devices are regularly scanned and have all security patches applied in a timely manner.

N. Researcher shall use a secure method such as Secure File Transfer Protocol (SFTP) or comparable method to transmit Data. Researcher shall never send Data via email or transport Data on removable media.

O. Researcher shall have physical security in buildings housing Data, along with controlled physical access to buildings and/or data centers.

P. Researcher's devices used to copy or scan hard copies of Data must have encrypted storage. Researcher shall scrub storage devices when equipment is retired. Hard copies containing Data are discouraged and must be physically secured, not left unattended, and physically Destroyed.

Q. Researcher shall protect Data stored in cloud-based systems in the same manner as local Data. Use of free cloud based services is prohibited. Data shall use secondary encryption to protect Data in cloud storage. Cloud environments, when employed by Researcher, must be fully documented by Researcher and open to USBE inspection and verification. Access to Researcher's cloud based computing environments is only permitted via restricted access, by VPN or least privileged access lists, and never accessible directly via the Internet.

VIII. Transparency Requirements

A. Researcher shall facilitate access to and correction of any factually inaccurate student data in response to a request from a LEA or from USBE.

B. Researcher acknowledges that USBE will post this Agreement to USBE's website.

IX. Data Governance Plans

A. Researcher agrees to have in place a Data Governance plan with support and participation from across the organization that details the organization's policies and procedures to protect privacy and data security, including ongoing management of data collection, processing, storage, maintenance, use, and destruction. USBE has the right to conduct audits or other monitoring of Researcher's Data Governance policies, procedures, and systems.

B. If, through these monitoring activities, vulnerability is found, Researcher must take timely appropriate action to correct or mitigate any weaknesses discovered. If Researcher's current data security policies and procedures are not posted on an externally facing website, they will be provided to USBE if requested and must include the minimum security policies and procedures set forth below:

1. Privacy and Security Policies and Procedures
2. Identification of a Privacy and Security Board and Officer
3. Management Oversight of Privacy and Security Programs

4. Sanctions for Violations of Policies and Procedures
5. Reporting Potential Problems in Privacy and Security
6. Incident Response and Incident Response Mitigation
7. Privacy and Security Training
8. Access Control, Minimum Necessary Access and Verification for Access to Data
9. Password Management
10. Transmitting Sensitive Information Securely including Faxing and Email
11. Log-in Monitoring
12. Workstation Security Configuration
13. Device and Media Control
14. Securing Materials with Data
15. Encryption
16. Authorizations for Personal Health Information, if applicable
17. Permitted Uses and Disclosures of PHI, if applicable
18. HIPAA Status, if applicable
19. Business Associate Status, if applicable
20. Designating Sensitive Information
21. Risk Assessments and Management
22. Change Control Procedures
23. Audit and Evaluation Procedures

X. Data Retention and Destruction

A. USBE may terminate this Agreement at any time, for its own convenience, for any reason, with written notice to the Requester. The Requester may terminate this Agreement for any reason, with 30 days written notice to the State.

B. Upon request by USBE made before or within thirty (30) calendar days after termination of the Agreement, Researcher shall make available to USBE a complete and secure (i.e. encrypted and appropriately authenticated) download file of all Data.

C. USBE retains the right to use the established operational services to access and retrieve Data stored on Researcher's infrastructure at its sole discretion.

D. Following the termination of this Agreement, Researcher shall, within thirty (30) calendar days, Destroy all Data collected, generated, or inferred as a result of this Agreement. Researcher shall certify to USBE in writing that the Data has been Destroyed.

XI. Individual Duties

A. Researcher agrees to obtain formal Institutional Review Board (IRB) approval.

B. All involved Data Owners will participate in the determination to provide Data based on USBE polices and applicable laws and regulations. Data Owners will also participate in any validation and risk assessments as defined in this Agreement.

C. The Data Owner takes ownership of the operational, technical, and informational management of the Data.

D. Each Party's Data Governance Manager is authorized, after following approved internal Data Governance policies, to approve the use of Data.

E. The Data Steward shall manage the source system, and ensure the integrity and safety of the Data at all times.

F. The Data Steward shall follow all security requirements outlined in this Agreement, to prevent the use or disclosure of Data not authorized by either this Agreement or the attached appendices.

G. The Data Steward agrees to abide by all applicable state and federal laws and regulations, including FERPA, HIPAA, Utah's Student Data Protection Act, and others as specified in attached Appendices.

XII. Data Linkage

A. If Researcher will link USBE's Data with Data from another source, the result could be a new data set with potentially unique regulations and conditions governing its use. Prior to linking the Data, Researcher will provide detailed information to USBE outlining the Data being linked and the other sources for Data.

B. The Data Steward will classify the linked data based on security or privacy risks. This could include evaluating the method of release, on the likelihood of identifying individuals from the linked Data, if linking the Data will violate any laws or regulations, or if the new data set meets the original request.

C. Based on the results of the risk assessment, USBE may refuse to provide Researcher with some or all of the requested Data in its sole discretion in order to mitigate any risks identified.

D. Should USBE consent to the Data being linked, the Data Steward shall apply additional constraints as necessary to the usage of the new data set.

E. Detailed information on the Data being linked, the other sources of Data, and any additional constraints shall be documented in the Appendix.

XIII. Unauthorized Uses, Disclosures or Breaches

A. If Researcher becomes aware of an Incident, misuse of Data, or unauthorized disclosure involving any Data, it shall notify the USBE within one (1) calendar day and cooperate with USBE regarding recovery and remediation of the Incident, and the necessity to involve law enforcement, if any.

B. Researcher shall determine the cause of an Incident and produce a remediation plan to reduce the risk of incurring a similar type of breach in the future. Researcher shall present its analysis and remediation plan to USBE within ten (10) calendar days of notifying USBE of an Incident. USBE reserves the right to adjust this plan, in its sole discretion. If Researcher cannot produce its analysis and plan within the allotted time, USBE, in its sole discretion, may perform such analysis and produce a remediation plan, and Researcher shall reimburse USBE for the reasonable costs thereof.

C. Unless Researcher can establish that Researcher is not the cause or source of the Incident, Researcher shall be responsible for the cost of notifying each person whose Data may have been compromised by the Incident.

D. Disclosure of Data by Researcher for any reason may be cause for legal action by third parties against Researcher, USBE, or their respective agents. Researcher shall indemnify, save, and hold harmless USBE, its employees, and agents against all claims, damages, liability, and court awards including costs, expenses, and attorney fees incurred because of any act or omission by Researcher, or its employees, agents, Subcontractors, or assignees pursuant to this Agreement. Notwithstanding any other provision of this Agreement, Researcher shall be liable to USBE for all direct, consequential, and incidental damages arising from an Incident caused by Researcher.

E. In the event of an Incident, Researcher shall provide USBE or its designated representatives with access seven (7) days a week, twenty-four (24) hours a day, for the purpose of evaluating, mitigating, or resolving the Incident.

XIV. Data Accuracy

A. The Data provided are the best and most complete documentation available. USBE does not ensure 100% accuracy of all records and fields. Some data fields, including those that are not used, may contain incorrect or incomplete Data. USBE and Researcher will report any systematic problems with the Data to the Data Owner. Data that has been manipulated or re-processed by either USBE or Researcher is the responsibility of that Party.

XV. No Financial Obligation

A. Except for the Researcher’s financial indemnity obligation to USBE in the case of damages caused by Researcher’s data security breach, this Agreement includes no additional financial terms. The terms of any financial liability that arises from data processing activities carried out in support of the responsibilities covered herein must be negotiated separately and to the mutual satisfaction of the Parties. Neither Party is authorized to enter into any arrangements or agreements for or on behalf of the other Party which could involve financial liability.

XVI. Survival

A. The respective rights and obligations of parties shall survive the termination of this Agreement with respect to Data previously shared.

XVII. Effective Date and Term

A. This Agreement shall take effect upon its signing by all Parties.
B. This Agreement may be amended at any time by mutual agreement of all Parties.
C. All parties will conduct an independent review of this Agreement on an annual basis.
D. This Agreement shall expire 12 months from the date of execution. It may be extended in yearly increments by mutual agreement of the parties up to a maximum term of 5 years. If a Party desires to extend this agreement, it must provide a notice of intent to renew no later than 90 days prior to expiration of the agreement. Under no circumstances shall the agreement be back dated or made to apply retroactively.

XVIII. Cost (OPTIONAL)

Researcher agrees to pay fees in the amount of $___for the preparation or delivery of the Research Data (this payment may be required in advance). Payment shall be made to: (If this provision is used, then Para. XV should be deleted for modified)

XIX. Signatures

To further the collection and analysis of Utah educational Data, USBE and Researcher agree to the cooperative sharing of Data between the Parties pursuant to the conditions set forth herein.

Signature: ______________________________ Date: ___/___/___

State Superintendent of Public Instruction

Utah State Board of Education

Signature: ______________________________ Date: ___/___/___

Title:

Requesting Organization