## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Chapter 1: Data Governance Plan</td>
<td>4</td>
</tr>
<tr>
<td>Chapter 2: Data Collection</td>
<td>6</td>
</tr>
<tr>
<td>Student Data Protection Act</td>
<td>6</td>
</tr>
<tr>
<td>Necessary Data Elements</td>
<td>6</td>
</tr>
<tr>
<td>Prohibited Data Elements</td>
<td>7</td>
</tr>
<tr>
<td>Optional Data Elements</td>
<td>8</td>
</tr>
<tr>
<td>PPRA and Utah FERPA</td>
<td>9</td>
</tr>
<tr>
<td>Chapter 3: Disclosures</td>
<td>12</td>
</tr>
<tr>
<td>FERPA Requirements</td>
<td>12</td>
</tr>
<tr>
<td>School Officials</td>
<td>13</td>
</tr>
<tr>
<td>Education Records</td>
<td>13</td>
</tr>
<tr>
<td>Sharing information with Department of Human Services</td>
<td>14</td>
</tr>
<tr>
<td>FERPA Exceptions</td>
<td>14</td>
</tr>
<tr>
<td>Data Privacy Agreements and Contracts</td>
<td>17</td>
</tr>
<tr>
<td>Online Educational Tools</td>
<td>17</td>
</tr>
<tr>
<td>Third-Party Audits</td>
<td>18</td>
</tr>
<tr>
<td>Flowchart to Guide Disclosures</td>
<td>19</td>
</tr>
<tr>
<td>Chapter 4: Metadata Dictionary</td>
<td>20</td>
</tr>
<tr>
<td>Chapter 5: Training</td>
<td>22</td>
</tr>
<tr>
<td>Chapter 6: Data Breach Response</td>
<td>24</td>
</tr>
<tr>
<td>Incident, Breach, Significant Breach</td>
<td>26</td>
</tr>
<tr>
<td>Involving Law Enforcement</td>
<td>27</td>
</tr>
<tr>
<td>Developing an Incident Response Team (IRT)</td>
<td>27</td>
</tr>
<tr>
<td>Typical members of an incident response team</td>
<td>28</td>
</tr>
<tr>
<td>Factors when determining team membership</td>
<td>28</td>
</tr>
<tr>
<td>Preventative Steps</td>
<td>29</td>
</tr>
<tr>
<td>Appendices</td>
<td>30</td>
</tr>
<tr>
<td>Appendix A - Definitions</td>
<td>31</td>
</tr>
<tr>
<td>Appendix B - Laws</td>
<td>33</td>
</tr>
<tr>
<td>Appendix C - Data Gateway</td>
<td>37</td>
</tr>
</tbody>
</table>

### Introduction

Utah is committed to protecting student data privacy. Doing so while enabling the use of data to improve educational outcomes and educational technology to transform educational experiences is challenging. In response to that challenge, the Utah State Board of Education’s (USBE) Student Data Privacy team was established. This guidebook was developed by the Student Data Privacy team as a resource to support Local Education Agencies (LEAs) and their data managers and is regularly updated to reflect changes in federal law, state law, USBE board rule, and best practices.

In this guidebook, each chapter will have an overview that includes requirements, steps and considerations, as well as resources available. This chart was developed in hopes of creating a quick reference with thorough guidance. Additionally, templates and exemplars are provided to help facilitate the work of LEAs and data managers. If clarification, a template, or additional guidance is needed, please reach out to the Student Data Privacy Team.
1 Data Governance Plan

Utah law, 53E-9-301(6), requires each local education agency (LEA) create a Data Governance Plan and annually post the plan on their website. The plan is intended to be a collection of the LEA’s policies related to protecting student data. The chart below indicates the legal requirements for your data governance plan as well as suggested annual activities.

The USBE Student Data Privacy section has a template, which meets all of the requirements of 53E-9-301(6). Sections in yellow indicate areas for additional detail of local policies. If using an older template from USBE, LEAs should update their data governance plan to reflect the most recent version. LEAs may use the entire template to create their plan or select the sections that are lacking in their current policies.

Each September, the USBE Student Data Privacy section will send a survey to LEAs which will allow LEAs to share evidence that they are compliant with all privacy requirements. Since the Data Governance Plan must be available on the LEA’s website, sharing the URL where the plan is located will suffice. The student data privacy auditor will review the plan in detail to ensure that it meets all of the requirements specified in 53E-9-301(6)(a)–(g). If any are missing, the auditor will coordinate with the data manager on how to incorporate the requirements into the LEA’s plan.

### Requirements

**Best Practices:** Incorporate reasonable data industry best practices to maintain and protect student data and other education-related data.

1. Adopt a cybersecurity framework.
2. Consider using the CIS Controls.
3. Ensure staff are prepared to follow the adopted framework.
4. Write the policy (describe the cybersecurity framework the LEA has adopted.)

**Roles & Responsibilities:** Describe the roles, responsibilities, and authority of data governance staff members.

1. Designate a staff member to be the Data Manager and a staff member to be the Information Security Officer.
2. Ensure staff are aware of their responsibilities.
3. Describe the LEA’s data governance roles.
4. Write the policy - Determine if there are additional staff performing data governance tasks such as records officer or others.

### Steps and Considerations

**Technical Support:** Provide the necessary technical assistance, training, support, and auditing.

1. Review the training section of the Data Governance Plan Template and this guidebook.
2. Determine what training the LEA would like to provide.
3. Review the audit section of the Data Governance Plan Template.
4. Develop an audit policy or leverage the audit policy of the Data Governance Plan Template.
5. Write the policy - Describe the LEA data governance training plan and audit policy.

**Sharing Data:** Describe the process for sharing student data between an education entity and another person.

1. Check for old data release policies.
2. Review the disclosure section of the Data Governance Plan Template and this guidebook.
3. Leverage the old data release policy, the LEA’s annual FERPA notice, or the language from the Data Governance Plan Template.
4. Write the policy - Describe the LEA’s disclosure process. If individuals other than the data manager approve data sharing, then clearly explain.

**Expungement:** Describe data expungement process, including how to respond to requests for expungement.

1. Review the Expungement Request Policy section of the Data Governance Plan Template.
2. If additional information is needed review 34 CFR 99, Subpart C of FERPA.
3. Write the policy - Clearly describe the LEA’s expungement process.

**Breach Response:** Describe the data breach response process.

1. Review the Breach Response section of the Data Governance Plan Template.
2. Review the Data Breach section of this guidebook.
3. Write the policy - Clearly describe the LEA’s breach response process.

**Publication:** Publish policy annually and make it available on website.

1. Publish plan annually.
2. Suggestions from LEAs:
   - Set up a data privacy section on LEA web site, which includes links to the plan, training materials, and the metadata dictionary.
   - Include within the parents’ guidebook or a general policy guidebook.

### Resources

- See Section 4 and 5 of the Data Governance Policy Template.
- See Section 4 and 5 of the Data Governance Policy Template.
- See Section 7 of the Data Governance Policy Template.
- See Section 8 of the Data Governance Policy Template.
- Example 1: Northstar Academy
- Example 2: Webster School District
Data Collection

Data about students is collected for important purposes like informing instruction and making decisions about resources needed to support students. This section addresses data collection including Utah’s Student Data Protection Act, Utah FERPA, and the Protection of Pupil Rights Amendment.

Student Data Protection Act

Student data privacy can be enhanced by limiting the amount of sensitive information a school collects. Utah’s Student Data Protection Act addresses this by classifying data in three ways:

1. prohibited (may never be collected or only in limited circumstances),
2. necessary (may be collected in all circumstances), and
3. optional (may only be collected with parental consent).

Additionally, the Student Data Protection Act improves transparency with parents by notifying them of the information that is being collected, the risks and benefits of such collections, how the data are kept secure, and what rights they have regarding the data collected.

### Necessary Data Elements

Non-exhaustive list of elements that are always considered necessary

- Name
- Date of birth
- Gender
- Parent contact information
- Custodial parent information
- Contact information
- Student identification number
- Local, state, and national assessment results or an exception from taking a local, state, or national assessment
- Course grades and grade point average
- Courses taken, completed, credits earned, and other transcript information
- Grade level and expected graduation date or graduation cohort
- Degree, diploma, credential attainment, and other school exit information
- Attendance and mobility
- Drop-out data
- Immunization record or an exception from an immunization record
- Race
- Ethnicity
- Tribal affiliation
- Remediation efforts
- Exception from a vision screening or information collected from a vision screening
- Information related to the Utah Registry of Autism and Developmental Disabilities
- Student injury information
- Disciplinary record created and maintained as described in Section 53E-9-306
- Juvenile delinquency records
- English language learner status
- Child find and special education evaluation data related to initiation of an IEP descriptions of a student

### Prohibited Data Elements

LEAs may not collect student social security numbers under any circumstances. Student criminal records may only be collected in accordance with 78A-6-112(3)(b), wherein if a student is taken into custody for a violent crime or a weapons offense, the law enforcement agent must notify the LEA’s superintendent or director.

### Requirements

<table>
<thead>
<tr>
<th>Ensure that prohibited student data are not collected.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Review the descriptions of prohibited, optional, and necessary data. <strong>(ANNUALLY)</strong></td>
</tr>
<tr>
<td>2. Develop an index of all data collected.</td>
</tr>
<tr>
<td>3. Ensure that prohibited data are not collected.</td>
</tr>
</tbody>
</table>

### Steps and Considerations

<table>
<thead>
<tr>
<th>Provide parents with an annual collection notification both via the school’s website and as a standalone document.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the model notification to create a notice that includes:</td>
</tr>
<tr>
<td>a list of the student data collected by the education entity (leverage index created);</td>
</tr>
<tr>
<td>a statement expressing that the education entity will not collect social security numbers or criminal records except in accordance with 78A-6-112(3)(b);</td>
</tr>
<tr>
<td>a statement indicating at the education entity will not share optional student data without written parental consent;</td>
</tr>
<tr>
<td>the following statement: “The collection, use, and sharing of student data has both benefits and risks. Parents and students should learn about these benefits and risks and make choices regarding student data accordingly.”;</td>
</tr>
<tr>
<td>a description in general terms explaining how the education entity stores and protects student data; and</td>
</tr>
<tr>
<td>student’s rights under this part. <strong>(ANNUALLY)</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Only collect data designated as optional with written parental consent.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Before collecting any additional data, review the data classifications.</td>
</tr>
<tr>
<td>2. If any optional data are desired, ensure the school is collecting parental consent. <strong>(ANNUALLY)</strong></td>
</tr>
</tbody>
</table>

### Resources

- See descriptions of the three types of data.
- Model Notification
- Sample Consent
The law specifies that the following are optional and require informed parental consent before collecting:

- Biometric Information
- Information related to an IEP or needed to provide special needs services (after the IEP has been initiated)
- Information required for a student to participate in an optional federal or state program (e.g., information related to applying for free or reduced lunch)
- Information that is not “Necessary Information” as defined in this guidebook

Biometric information is always considered an optional collection under Utah law and will require written parental consent. There are two criteria that must be met for data to be considered biometric information:

1. The collection must contain a biometric identifier and
2. Be used for the purposes of identifying a student.

Utah law gives a very specific list of biometric identifiers, which are:

- Retina or iris scan
- Fingerprint
- Human biological sample for valid scientific testing or screening
- Scan of hand or face geometry

Non-biometric identifiers are writing samples, written signatures, voiceprint, photographs, demographic data, or physical.

If you find a data element that is not on the included lists, please consult with the Student Data Privacy section. We will work with our various stakeholder groups to determine the most appropriate course of action.

PPRA and Utah FERPA

Teachers and schools are in positions of power when it comes to soliciting information from students. As such, laws have been passed at both the federal level (the Protection of Pupil Rights Amendment, or PPRA; 20 USC 1232h and 34 CFR 98) and state level (Utah FERPA; 53E-9-203), which are designed to ensure transparency, protect parental rights, and protect student privacy in cases where sensitive information might be collected.

PPRA and Utah FERPA require explicit parental consent before students can participate in any psychological or psychiatric examination, test, or treatment or survey, analysis, or evaluation covering any of the eight sensitive topics below.

- Political affiliations or philosophies
- Mental or psychological problems
- Sexual behavior, orientation, or attitudes
- Illegal, anti-social, self-incriminating, or demeaning behavior
- Critical appraisals of individuals with whom the student or family member has close family relationships
- Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers
- Religious affiliations or beliefs
- Income, except as required by law

Psychological or psychiatric examination, test, or treatment are not defined in Utah law, but are defined in the regulations for PPRA (see 34 CFR 98.4).

- Psychiatric or psychological examination or test means a method of obtaining information, including a group activity, that is not directly related to academic instruction and that is designed to elicit information about attitudes, habits, traits, opinions, beliefs or feelings.
- Psychiatric or psychological treatment means an activity involving the planned, systematic use of methods or techniques that are not directly related to academic instruction and that are designed to affect behavioral, emotional, or attitudinal characteristics of an individual or group.
Develop PPRA policy in consultation with parents for:
- Collecting parental consent if a psychological examination (test or treatment), survey, analysis, or evaluation collects information on one of the eight sensitive categories.
- The types of physical examinations or screenings the school may administer.
- The collection and use of personal information for the purpose of marketing information to student.

1. Review existing policies that might cover PPRA
2. Work with parents to develop necessary policies

Example 1: Juab School District
Example 2: Jordan School District
Example 3: Weber School District

Annually notify parents of anticipated dates of collection and of their rights under PPRA.
1. Right to inspect and review materials.
2. Right to not participate.
3. Right to inspect the instrument or materials related to the examination or treatment at the school.
4. The URL where a copy of the survey can be found, if applicable.
5. Right to request any of the following:
   - records or information, including information about relationships, that may be examined or requested;
   - The means by which the records or information shall be examined or reviewed;
   - the means by which the information is to be obtained;
   - the purposes for which the records or information are needed; or
   - the entities or persons, regardless of affiliation, who will have access to the personally identifiable information.

1. Work with staff to ensure all possible surveys, examinations, and other covered activities are known to administration. (ANNUALLY)
2. Develop notice to be delivered annually at the beginning of the school year and again during the year if there is any change to policy. (ANNUALLY)
3. Ensure notice is “direct notice”, meaning notification must be provided by hand, email, or postal mail. Having notice on your website is insufficient. (ANNUALLY)

Note: Utah FERPA specifies that consent would still be required, whether the information is personally identifiable or not. Additionally, notification must occur at least two weeks prior to any event.

Collect written parental consent prior to any activity covered under the policy.

Provide in-service training for teachers and administrators regarding the policy.

Note: The law does not restrict a student’s free speech rights. Students are freely allowed to spontaneously express sentiments or opinions related to the eight sensitive topics. Furthermore, if a school employee believes a student is at risk of suicide, physical self-harm, or harm to others, then the school employee may intervene and ask questions that may touch upon the eight sensitive topics to refer them to the appropriate prevention services and to inform the parent. Utah law further specifies that the school should have a policy requiring the minimum degree of intervention possible to accomplish this goal.
As part of day-to-day functions for a school or district, student data will need to be disclosed to a variety of individuals, ranging from classified and certified staff to contractors and researchers. FERPA provides guidelines as to when it is reasonable for the school to share student data and establishes restrictions to ensure transparency and control so as to protect student privacy. This chapter addresses FERPA requirements, FERPA exceptions, data privacy agreements, and audits.

## FERPA Requirements

The following outlines FERPA requirements related to disclosing student data.

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Steps and Considerations</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine who constitutes a school official with legitimate educational interest.</td>
<td>Review the school officials’ section. Determine who will be considered a school official. Include this information in the annual parental notification of FERPA rights.</td>
<td>School Official Section, Model Annual Notification</td>
</tr>
<tr>
<td>Determine which data will be considered directory information.</td>
<td>Directory information is information that is generally considered to not be harmful. Name, address, telephone number, date and place of birth, participation in officially recognized activities and sports, and dates of attendance are often considered directory information.</td>
<td>USBEd Video PTAC Video</td>
</tr>
</tbody>
</table>
| Provide parental notice of directory information. | 1. Develop a notification including the following:  
   - The list of data elements that are considered directory information.  
   - The parent’s or eligible student’s right to opt out of all or part of directory information.  
   - The time period the parent or eligible student has to provide a written opt-out of all or part of the directory information.  
   2. Track opt-outs and honor them. In practice, your Student Information System (SIS) may have this ability, or in some cases, you can track them in a spreadsheet.  
   3. Your directory information policy does not have to be an all or nothing policy, and some LEAs chose to have more of an a la carte policy (e.g., it is common for the yearbook or a classroom website to be listed separately.) | Model Directory Information Notification |

### School Officials

School officials include educators and other staff that work for the school; however, not every employee should have access to all student information. For an internal school official to receive student data, they must have legitimate educational interest; that is, you need to determine who needs the information for their job and restrict their access to records where there is no legitimate educational interest.

Outside parties (contractors, consultants, volunteers) may also be designated school officials, but there are a few more rules. Namely, they must perform an institutional service or function for which you would otherwise use employees; they must be under the direct control of the LEA with respect to the use and maintenance of education records; and they must not redisclose PII from the records.

Regardless of whether the school official is an internal or an outside party schools must take reasonable methods to ensure only those with a legitimate educational interest receive access to records. Reasonable methods could include physical controls (locks), technical controls (log in credentials), or administrative controls (contracts or policies). Note that under Utah law, when contracting with a third-party, there are certain provisions required in the contract beyond the FERPA requirements. See the Contracts chapter of this guidebook for more details.

### Education Records

The requirements of FERPA only apply to education records. To be considered an education record, the data must directly relate to the student and must be maintained by the school or an agent of the school. Some examples of cases that are not education records are as follows:

- Surveillance video footage where the student is just a bystander (i.e., it does not directly relate to the student)
- Peer-graded classroom assignments (i.e., they are not maintained by the school)
- Personal notes kept by a school official used as a memory aid and not shared with others
- Records created, maintained, and used by a designated law enforcement unit (note that this is not the default, and records created and maintained by on campus law enforcement will be covered by FERPA unless you specifically designate it as separate under policy)
Sharing Information with the Department of Human Resources

LEAs should share information with the Department of Human Services (DHS) and its divisions using FERPA’s caseworker exception. This exception states that the DHS agency may have access to student records once the child is under the care and protection of the agency. Utah law specifies that if a caseworker is investigating a case of educational neglect, then the criteria has been met. Note that DHS consists of several divisions. The divisions most likely to be involved with schools are Child and Family Services (DCFS), Juvenile Justice Services (JJS), and Systems of Care (SOC).

FERPA Exceptions

Without parental consent, a FERPA exception is required to share student data. The chart below identifies common exceptions and indicates if a data privacy agreement (DPA) is needed.

<table>
<thead>
<tr>
<th>Exception</th>
<th>Steps and Considerations</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health and Safety</td>
<td>1. Determine if there is an articulable and significant threat to the health or safety of the student or other individuals. 2. If there is a threat, notify appropriate officials.</td>
<td>34 CFR 99.31(a)(10)</td>
</tr>
<tr>
<td>State and local authorities within a juvenile justice system</td>
<td>1. Determine if the student is guilty of an infraction described in U.C.A. 53G-8-211(3). 2. Refer the student to an evidence-based alternative intervention.</td>
<td>34 CFR 99.31(a)(5)</td>
</tr>
<tr>
<td>Financial Aid</td>
<td>1. A DPA is advised. 2. See DPA and contract section.</td>
<td>Financial aid language for contracts section</td>
</tr>
<tr>
<td>Contractors (school official exception)</td>
<td>Third-party contractors are defined broadly in Utah law to include any individual or organization that collects or receives student PII in order to provide a service. 1. When using the contractor or school official exception; • they must perform an institutional service or function for which you would otherwise use employees; • they must be under the direct control of the LEA with respect to the use and maintenance of education records; • and they must not redisclose PII from the records. 2. A DPA or contract is required.</td>
<td>34 CFR 99.31(a)(1)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Exception</th>
<th>Steps and Considerations</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>School Officials</td>
<td>1. Must have a legitimate educational interest. 2. Include in FERPA annual notification.</td>
<td>34 CFR 99.31(a)(1)</td>
</tr>
<tr>
<td>Directory Information</td>
<td>1. Determine what information will be directory information. 2. Include in directory information notification. 3. Companies that provide services related or similar to school photography, yearbooks, or graduation announcements usually fall under this exception.</td>
<td>34 CFR 99.31(a)(11)</td>
</tr>
<tr>
<td>Schools to which the Student is transferring</td>
<td>Student’s parents must be notified of the transfer, receive a copy of the record if desired, and have an opportunity for a hearing to challenge the content of the record.</td>
<td>34 CFR 99.31(a)(2)</td>
</tr>
<tr>
<td>Judicial order or lawfully issued subpoena</td>
<td>1. Make a reasonable effort to notify the parent or eligible student of the order or subpoena in advance of compliance. 2. Provide information requested in the order.</td>
<td>34 CFR 99.31(a)(9)</td>
</tr>
<tr>
<td>Exception</td>
<td>Steps and Considerations</td>
<td>Resources</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Studies for, or on behalf of, a school</td>
<td>1. Ensure the work meets one of the three applicable purposes. Studies for, or on behalf of, the school can only be used to • develop, validate, or administer predictive tests; • administer student aid programs; or • improve instruction. 2. Per Utah law, develop an external research review process that ensures • the research meets the requirements of FERPA’s studies exception and • there is a valid written agreement in place between the LEA and the researcher. 3. A DPA is required that • includes the purpose, scope, and duration of the study along with the PII to be disclosed; • requires the researcher to only use the PII for the purposes stated in the agreement; • requires the study to be conducted in a way that doesn’t permit identification of individuals by anyone other than those designated by the researcher; and • requires the researcher to destroy the PII at the end of the study.</td>
<td>34 CFR 99.31(a)(6) Studies agreement language</td>
</tr>
<tr>
<td>Audit or evaluation of federal or state supported education program</td>
<td>A DPA is required that • designates the individual or entity as an authorized representative; • specifies the PII to be disclosed and the purpose of the audit/evaluation; • describes the work to be done along with how the PII will be used; • requires the authorized representative to destroy all PII at the end of the audit/evaluation and specifies the time period for disposition; and • establishes policies and procedures to ensure that PII is only available to those with legitimate educational interests.</td>
<td>34 CFR 99.35 Audit and evaluation language</td>
</tr>
</tbody>
</table>

**Data Privacy Agreements and Contracts**

Data privacy agreements, at a minimum, require: a purpose, a list of data elements, a restriction of use, and terms of data destruction. Utah’s Student Data Protection Act requires the following provisions when entering an DPA or any agreement with a third-party contractor:

- requirements and restrictions related to the collection, use, storage, or sharing of student data;
- a description of the types of affiliates with whom the contractor can share student data;
- provisions that govern deletion of student data at the LEA’s request;
- prohibitions on the secondary use of student data; and
- an agreement that the LEA or its designee may audit the contractor to verify compliance with the contract.

USBE has developed a Data Privacy Agreement, or DPA, that meets FERPA and Utah State Privacy laws. When vendors sign the Agreement, it makes the Utah DPA essentially a piggy-backable or umbrella agreement, requiring only the signature of the additional LEA to make it binding and eliminating any further privacy negotiations for that resource.

Additionally, USBE has partnered with the Student Data Privacy Consortium to create a Utah Privacy Alliance website that can house all privacy agreements. To gain access to this page, you will need to complete an onboarding training before receiving your login information. You can request this training by emailing privacy@schools.utah.gov.

Please note when sharing de-identified data, a DPA or contract is not required since the third-party contractor would no longer be receiving student PII; however, please note that PII includes identifiers such as student ID numbers and SSIDs. If you are sending these identifiers, you are still sharing PII, and therefore, must establish a DPA that includes the contract requirements.

**Online Educational Tools**

When sharing student data with online education providers, a terms of service agreement also qualifies as a contract. This means that when sharing student data with websites that are specifically intended for K-12 students, you are entering a contract, which will have to include the contract requirements identified above.

If the website or app is intended for general audiences (e.g., websites and apps that are not specifically targeting K – 12 education), you are not required to follow the contract requirements. Adobe Creative Cloud, for example, is specifically intended for a professional context, whereas ClassDojo is only used in schools.
Third-Party Audits
Utah’s contract requirements include a right-to-audit clause. Third-party contractors might be wary of the potential scope of any audits and might want more specificity as to what an audit might look like. First, the audits should only be in relation to verifying compliance with the privacy and security requirements of the contract. It does not need to cover finances or other aspects of the third-party contractor’s business (unless that is agreed upon). Furthermore, audits do not have to be performed onsite.

As described in R277-487-7, an audit could simply be the third-party contractor providing the LEA a self-assessment of their compliance, responses to a questionnaire provided by the LEA, or a report of an industry-recognized privacy and security audit. Some businesses may also have an independent audit completed, leading to a System and Organization Controls (SOC) 2 or 3 report. The difference between these reports is that a SOC 3 is for general use and may be freely distributed, though a third-party contractor may agree to share a SOC 2 with you. If the third-party contractor can share one of these reports with you, it would also meet the audit requirements.
FERPA requires that schools provide parents with the opportunity to inspect and review all student records maintained by school officials—including third-party contractors, such as websites. Furthermore, parents have a right to receive a reasonable explanation or interpretation of the records, including their purpose. The Student Data Protection Act is similar in that it requires this information be available on demand in an online “metadata dictionary”. The Metadata Dictionary should:

• Define and disclose all student PII the LEA collects and shares,
• Comprehensively list all recipients with whom you share student PII, including:
  - the purpose for sharing,
  - the justification for sharing (including if it is required by federal or state law), and
  - why the sharing is permitted under Federal and State law (what FERPA exceptions allow the release or indicate that written parental consent was obtained.)

The Student Data Protection Act requires that Metadata Dictionary entries be posted in a way where a student cannot be identified. You may interpret this to mean data disclosures that only impact individual students or disclosures with very small n sizes (n < 10 is a good standard) should not have entries in the Metadata Dictionary. Additionally, some data will almost always fall under this category and should not be disclosed; therefore, they are not included in the tool. These data are: financial aid, health/safety emergency, case workers, and sex offenders. Furthermore, since some FERPA exceptions require LEAs to notify parents of a disclosure, there is no need to include these disclosures in the Metadata Dictionary, and therefore, these data categories are not available in the tool. These are student transfer, dependent student, and subpoena or court order.

Each year, the LEA will submit to USBE evidence that the Metadata Dictionary has been completed for the year. This evidence will be a statement certifying that the dictionary is complete and accurate as of October 1. LEAs will also submit a description of the process used to gather the information to be entered into the tool.

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Steps and Considerations</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain a Metadata Dictionary</td>
<td>Enter information identified in the steps below to a metadata dictionary.</td>
<td>Data Gateway</td>
</tr>
<tr>
<td>Enter data elements in the Metadata Dictionary</td>
<td>Begin by entering all the data elements that you are sharing and with whom you are sharing them.</td>
<td>Guidance in this section</td>
</tr>
<tr>
<td>Include in the Metadata Dictionary the purpose for sharing the data element</td>
<td>Enter a short explanation in the description field that describes the purpose for sharing the data.</td>
<td>Guidance in this section</td>
</tr>
<tr>
<td>Include in the Metadata Dictionary the justification for sharing the data element</td>
<td>Use the Federal or State Justification, Justification Name, and URL fields. Note: If the justification comes from a federal or state law, USBE will populate these fields. LEA may modify these entries should they choose to add any locally-pertinent information. Otherwise, LEAs will only be expected to enter those justifications that are based on a local or other directive.</td>
<td>Guidance in this section</td>
</tr>
<tr>
<td>Include in the Metadata Dictionary why sharing the data element is permitted under federal and state law</td>
<td>1. Determine one or more FERPA exceptions that are being followed that permit the release or indicate that written parental consent was obtained. 2. Indicate appropriate FERPA exception in the FERPA Exceptions box.</td>
<td>FERPA exceptions / Guidance in this section</td>
</tr>
<tr>
<td>Display the Metadata Dictionary on LEA website</td>
<td>Provide a link to the dictionary on the LEA’s website.</td>
<td>Guidance in this section</td>
</tr>
</tbody>
</table>
## Training

In order to ensure that data privacy policies are followed, educators and staff that have access to student personally identifiable information should have regular training opportunities. The following table shows all of the required privacy trainings. (Please see USBE’s YouTube playlist to support training initiatives.)

### Delivered by USBE

<table>
<thead>
<tr>
<th>Training</th>
<th>Audience</th>
<th>Frequency</th>
<th>Information to be Communicated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security and Privacy re-licensure training R277-487-14(3)</td>
<td>Licensed educators</td>
<td>When re-licensing (every 3–5 years)</td>
<td>Online Course</td>
</tr>
<tr>
<td>Note: This training can meet the annual training requirements of Utah FERPA and Student Privacy Act</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Delivered by the LEA

<table>
<thead>
<tr>
<th>Training</th>
<th>Audience</th>
<th>Frequency</th>
<th>Information to be Communicated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utah FERPA in-service 53E-9-203(8)</td>
<td>Teachers and administrators</td>
<td>Recommended when onboarding new employees</td>
<td>Overview</td>
</tr>
<tr>
<td>Student Privacy Act – training on student privacy laws 53E-9-204(3)(a)</td>
<td>School employees who are authorized to access student education records</td>
<td>Recommended when onboarding new employees - Must maintain a list of those trained and their signature.</td>
<td>Overview</td>
</tr>
<tr>
<td>Confidentiality of student data R277-487-3(20)</td>
<td>Employees with access to student records</td>
<td>Annually</td>
<td>Local policies on approved and unapproved disclosures. Be sure to include local policy found in your data governance plan.</td>
</tr>
<tr>
<td>• Who is your Data Manager and his/her responsibilities?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• How your LEA determines who has a legitimate educational interest in a student’s record?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Which elements are included in your directory information policy and when they are allowed to share directory information?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Where they can find which students have opted out of directory information?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• LEA process for approving websites and other online services for classroom use.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Data Breach Response

Data breach notification laws first appeared in the 2000s in response to concerns of identity theft. These laws generally require an institution to notify individuals if certain financial information were stolen giving individuals the opportunity to freeze their credit or take other protective action. A few of the reasons data breach response is important for school districts are listed below.

Protect the school’s reputation: In the event of a significant breach, you want to make sure you control the message.

Keep parents in the loop: Whereas student data likely cannot be monetized the same way financial data can, there are ways it can be used to harm students. For example, in the Dark Overlord attacks of 2018, parents received text messages with death threats based on data stolen from the school. In this case, notifying parents would help them know about the threat and how best to react to it.

Ensure that the school will take security and privacy seriously: One purpose of a breach response plan is to ensure that the LEA takes reasonable preventative methods to keep a breach from happening in the first place.

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Steps and Considerations</th>
<th>Resources</th>
</tr>
</thead>
</table>
| Have a breach response process as part of your data governance plan. | 1. Review resources and examples of breach response plans such as PTAC’s checklist and the plan included in the USBE’s model data governance plan.  
2. Work with your team to develop your response plan. | Data Breach Response Checklist by the Privacy Technical Assistance Center (PTAC)  
Data breach policy in the model data governance plan |
| Notify parents and adult students in the case of a significant data breach. | 1. Notify parents as soon as an incident has been declared a significant breach. (note: if law enforcement is involved be sure to consult with them first.)  
2. Include the following in the notification.  
   • A description of the incident  
   • The personally identifiable student data involved in the breach  
   • Steps the LEA is taking to stop the breach and prevent future incidents  
   • Steps that the parent or student may take to mitigate risks associated with the breach  
   • Contact information for individuals the parent can reach out to for more information or redress. This likely will include the LEA’s data manager and the Family Policy Compliance Office at the US Department of Education  
3. Deliver the notification to parents in a formal fashion (e.g., official letterhead and via postal mail.) | R277-487 defines “significant” |
| Notify USBE of significant data breaches within 10 business days. | Reach out to USBE’s Chief Privacy Officer or call 801-538-7500 for notification. | R277-487 defines “significant” |
Incident, Breach, Significant Breach

The Student Data Protection Act defines a data breach as an “unauthorized release of or unauthorized access to personally identifiable student data that is maintained by an education entity” [53E-9-301(6)]. Additionally, R277-487 establishes the standards an LEA should use to determine if a breach is significant. The flowchart below will help you determine if the incident is a breach and if it is significant.

1. Has there been an unauthorized release or access to personally identifiable data? (e.g., a hacker has gained access to a database where student personally identifiable information is held.)

2. Was the release unintentional? (e.g., a teacher downloaded student data to her personal computer)

Involving Law Enforcement

Many security incidents do not result in convictions largely because law enforcement are not notified. Depending on the nature of the incident, you may want to contact a different level of law enforcement. For example, if hardware is stolen from your facilities, then local law enforcement should be notified. Bear in mind, however, that once they are contacted, they may take over the entire investigation (confiscating affected hardware in the process.) As such, you should generally make sure you have concluded as much of your own investigation as possible before reaching out to local law enforcement. As a best practice, we recommend that you reach out to your local law enforcement before an incident occurs to discuss when and how this notification should be performed. This is also a good time to set up clear expectations.

Nearly all incidents that occur over the internet will fall under the jurisdiction of the FBI. In this case, we recommend you file a complaint with the FBI’s Internet Crime Complaint Center (IC3) at their website.

Developing an Incident Response Team (IRT)

One of the earliest steps you should take in preparing for a breach is designating an incident response team (IRT). The IRT will likely look very different from one LEA to another due to staffing and even geography issues. The following is intended as guidance to help you determine who should be selected as a team member on your IRT.

Typical members of an incident response team

The following business areas are generally represented on an LEA’s IRT:

- Management (superintendent, school director)
- IT Security Manager
- IT support (network administrators and those who have expert knowledge of the system)
- Legal (for determining your obligations and liability under the law)
- Public affairs/media relations (for determining how to handle all notifications)
- Business continuity planning (if the breach interrupts your ability to provide services to students, as in a denial of service attack, you will need to determine how to continue providing students with services)
- Human resources (in cases where employees are suspected of causing an incident)
- Facilities management (in cases where the data breach occurred via a physical security breach)
Factors When Determining Team Membership

Full time or outsourced
For a larger LEA, there may be multiple full-time employees covering each business area. For a smaller LEA or a charter school, many of these functions may be outsourced. In some cases, this will be to another state agency (e.g., a regional service center that handles network administration). In others, it may be a private firm. For example, many charter schools have completely outsourced their IT security with an external vendor.

LEAs that will be partially or completely outsourcing their response should make it clear in their policy which individuals or organizations will be filling these roles and how they will be communicating in the event of a breach, particularly if their offices are located far away from the LEA. You should also make sure that their breach response policies align with your expectations.

Availability
Another factor to consider is the availability of your staff. For example, your entire IT department may end up being members of the IRT, but you may not have the luxury to take them away from their regular duties simply because an incident is suspected. Some members, as such, may serve a part-time role on your IRT, providing their expertise when needed and continuing their normal duties to keep the LEA functioning.

Centralized or Distributed
Some agencies have a central team that handles the breach response. Due to staffing and geographic issues, some LEAs may have to opt for a more distributed approach. For example, the districts that cover larger counties (e.g., Emery, San Juan) may need to account for breaches that take place far away from the district office. In these cases, having a distributed model or even multiple IRTs governed by a centralized team might make more sense.

Preparation
Your data breach response plan should be useful to guide you in resolving incidents and breaches that occur, not just as a box to check off to demonstrate your compliance. The only way to really tell if the plan is a useful tool is to put it to the test, review take away lessons, and make updates to the plan to make it more useful.

The Student Data Privacy Section at USBE provides regular trainings on a variety of privacy/security topics to LEAs at their request. One of these trainings that could be requested is a breach response role play, wherein we would walk through a scenario with the LEA’s IRT. For more information, please contact the Student Data Privacy section.

If you would prefer to role play a breach on your own, PTAC has provided a data breach response training kit to role play a scenario with your IRT. The given scenario can be completed in roughly 1 – 2 hours. Another resource is the Computer Security Incident Handling Guide from the National Institute of Standards and Technology (NIST). Appendix A of the document covers multiple scenarios that could be used to stage a breach response roleplay.

Preventative Steps
As a best practice, we recommend that you include clear language in policy to indicate what educators, staff, and volunteers should expect; that is, which behaviors will not be tolerated, such as the following.

1.1 If an educator or staff recognizes that they have inadvertently sent student data to the wrong recipient, they will immediately contact the recipient, explain the mistake, and request that the data be deleted. If the recipient obliges and confirms, the LEA will not consider this a breach.

1.2 Educators and staff who are given access to LEA data systems should only access information as needed to complete their professional responsibilities. They should never be accessed for any personal or commercial purpose. Educators and staff who knowingly and intentionally violate this policy may be subject to school discipline.

1.3 An outboarding employee shall return all hardware to the LEA and certify in writing that all confidential student information has been destroyed on any personal devices. If the employee knowingly or intentionally takes confidential student information after certifying, this will be considered a breach and subject to misdemeanor penalties as described in 53E-9-310(1)(e).

1.4 Teachers may only store student data on the shared network and should not use thumb drives or similar unencrypted devices to store student data. This procedure will be included in the required annual privacy/security training given to staff each year. If the employee knowingly or intentionally stores confidential student information on an unencrypted device after receiving the training, this will be considered a breach and subject to misdemeanor penalties as described in 53E-9-310(1)(e).

1.5 Teachers may only share student data with a website or application if they have received parental consent or it has gone through the LEA’s app vetting process.
Defnitions

Data Breach: A data breach is the intentional or unintentional release of secure information to an untrusted environment.

Data Governance: The overall management of the availability, usability, integrity, and security of data used in an enterprise. A sound data governance program includes a governing body or council, a defined set of procedures and a plan to execute those procedures.

Direct Identifier: Direct identifiers include information that relates specifically to an individual such as the individual’s residence, including for example, name, Social Security Number, or other identifying number or code, email address, or biometric record.

Directory Information: Directory information is information that is generally considered to not be harmful. Name, address, telephone number, date and place of birth, participation in officially recognized activities and sports, and dates of attendance are often considered directory information.

Disclosure: Disclosure means to permit access to or the release, transfer, or other communication of personally identifiable information by any means. Disclosure can be authorized, such as when a parent gives written consent to share education records with an authorized party. Disclosure can also be unauthorized or inadvertent. An unauthorized disclosure can happen due to a data breach or a loss, and an accidental disclosure can occur when data released in public aggregate reports are unintentionally presented in a manner that allows individual students to be identified.

Education Record: The requirements of FERPA only apply to education records. To be considered an education record, the data must directly relate to the student and must be maintained by the school or an agent of the school. Some examples of cases that are not education records are as follows:
- Surveillance video footage where the student is just a bystander (i.e., it does not directly relate to the student)
- Peer-graded classroom assignments (i.e., they are not maintained by the school)
- Personal notes kept by a school official used as a memory aide and not shared with others
• Records created, maintained, and used by a designated law enforcement unit (note that this is not the default, and records created and maintained by on-campus law enforcement will be covered by FERPA unless you specifically designate it as separate under policy.)

Opt-out: Refers to the situation where parents choose NOT to participate. Data is shared unless the parent requests that it not be shared.

Opt-in: Refers to a situation where parents choose to participate. Data is ONLY shared if the parent consents to the sharing by signing a consent form.

Parental Consent: Parental consent means that the parent or legal guardian has been fully informed of the records to be disclosed, the purpose of the disclosure, and the individual or group receiving the student data. Consent should be signed and dated.

Personally Identifiable Information (PII): PII includes information that can be used to distinguish or trace an individual’s identity either directly or indirectly through linkages with other information.

School Officials: School officials include educators and other staff that work for the school; however, not every employee should have access to all student information. For an internal school official to receive student data, they must have legitimate educational interest; that is, you need to determine who needs the information for their job and restrict their access to records where there is no legitimate educational interest.

Suppression: Suppression is a disclosure limitation method which involves removing data (e.g., from a cell or row in a table) to prevent the identification of individuals in small groups or those with unique characteristics.

Appendix

Children’s Internet Protection Act (CIPA)
The Children’s Internet Protection Act (CIPA) is a federal law that applies to LEAs, schools, and libraries that receive discounted telecommunications, such as Internet access or internal connections, through the E-Rate program. CIPA requires LEAs to have an Internet safety policy and technology to block access to obscene or harmful content. LEAs must also monitor their students’ online activities and educate them on appropriate online behavior.

The Internet safety policy must address the following five components:

• Access by minors to inappropriate matter on the Internet
• The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communication (including instant messaging)
• Unauthorized access, including so-called “hacking” and other unlawful activities by minors online
• Unauthorized disclosure, use, and dissemination of personal information concerning minors
• Measures restricting minors’ access to materials harmful to minors.

Prior to adoption of the policy, CIPA requires public notice and at least one public hearing be held to address the proposed Internet Safety Policy. Most Internet Safety Policies are folded into an LEA’s acceptable use policy for students.

Children’s Online Privacy Protection Act (COPPA)
The Children’s Online Privacy Protection Act (COPPA) is a federal law governed by the Federal Trade Commission (FTC). COPPA assures that children under 13 years of age do not share personal information on the Internet without the express approval of their parents.

Providers must obtain consent from parents to collect information, unless they are collecting on behalf of the LEA or school and will only use the information to provide services to the LEA or school. If this is the case, then the provider can rely on consent obtained from the LEA or school. LEAs can consent on behalf of a parent for educational purposes.

COPPA defines personal information as:

• A first and last name
• A home or other physical address including street name and name of a city or town
Online contact information as defined in this section
A screen or user name where it functions in the same manner as online contact information, as defined in this section
A telephone number
A social security number
A persistent identifier that can be used to recognize a user over time and across different websites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier
A photograph, video, or audio file where such file contains a child’s image or voice
Geolocation information sufficient to identify street name and name of a city or town
Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described above.

FTC-Recommended Best Practices
• Allow parents to review the personal information collected.
• Ensure operators delete a student's personal information once the information is no longer needed for its educational purpose.
• Notify parents about the websites and online services to which it has provided consent on behalf of the parent concerning student data collection, as well as the operators’ direct notices. This information or a link to this information can be maintained on the LEA website.

Family Educational Rights and Privacy (FERPA)
The Family Educational Rights and Privacy Act (FERPA) is a federal law that affords parents the right to have access to their children’s education records, to seek to have the records amended, and to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student.

Generally, written permission from the parent or eligible student in order to release any information from a student’s education record. However, FERPA allows records to be disclosed without consent under the following conditions:
• School officials with legitimate educational interest
• Other schools to which a student is transferring
• Specified officials for audit or evaluation purposes

• Appropriate parties in connection with financial aid to a student
• Organizations conducting certain studies for or on behalf of the school
• Accrediting organizations
• To comply with a judicial order or lawfully issued subpoena
• Appropriate officials in cases of health and safety emergencies
• State and local authorities, within a juvenile justice system, pursuant to specific state law.

FERPA Regulations
Sample Notification
Directory Notification Sample

Protection of Pupil Rights Amendment (PPRA) - Utah FERPA (UTFERPA)
PPRA/Utah FERPA affords parents of elementary and secondary students certain rights regarding the conduct of surveys, collection and use of information for marketing purposes, and certain physical exams. These include, but are not limited to, the right to:
Consent before students are required to submit to a psychological or psychiatric examination, test, or treatment, or any survey, analysis, or evaluation in which the evident intended effect is to cause the student to reveal information concerning one or more of the following protected areas about the student or any family member (“protected information survey”) except as part of a suicide prevention program as described in 53G-9-702, if the protected information survey is administered by the state of Utah, or if there is a reasonable belief that there is an emergency, child abuse, neglect, or a serious threat to the well-being of the student.

1. Political affiliations or beliefs of the student or student’s parent;
2. Mental or psychological problems of the student or student’s family;
3. Sex behavior, orientation, or attitudes;
4. Illegal, anti-social, self-incriminating, or demeaning behavior;
5. Critical appraisals of others with whom respondents have close family relationships;
6. Legally recognized privileged relationships, such as with lawyers, doctors, or ministers;
7. Religious practices, affiliations, or beliefs of the student or student’s parent; or
8. Income, other than as required by law to determine program eligibility.

Receive notice and an opportunity to opt a student out of –
1. Any protected information survey that is part of a suicide prevention program described in 53G-9-702;
2. Any protected information survey administered by the state of Utah.
3. Any non-emergency, invasive physical exam or screening required as a condition of attendance, administered by the school or its agent, and not necessary to protect the immediate health and safety of a student, except for hearing, vision, or scoliosis screenings, or any physical exam or screening permitted or required under State law; and

4. Activities involving collection, disclosure, or use of personal information collected from students for marketing or to sell or otherwise distribute the information to others. (This does not apply to the collection, disclosure, or use of personal information collected from students for the exclusive purpose of developing, evaluating, or providing educational products or services for, or to, students or educational institutions.)

*Inspect, upon request and before administration or use* —

1. Protected information surveys of students and surveys created by a third party;
2. Instruments used to collect personal information from students for any of the above marketing, sales, or other distribution purposes; and
3. Instructional material used as part of the educational curriculum.

These rights transfer from the parents to a student who is 18 years old or an emancipated minor under State law.

---

**Student Data Protection Act**

Under this law, LEAs are required to adopt policies to protect student data and designate a data manager. They are also required to create and maintain a data governance plan, a metadata dictionary, and establish an external research review process. LEAs need to classify student data as necessary, optional, and prohibited and notify parents of their data policies. Schools may only collect optional data, such as biometric identifiers, with parental consent. When contracting with a third-party contractor who will use student personally identifiable information, the education entity shall require certain provisions in the contract.

**Student Privacy Act**

The Student Privacy Act requires that LEAs provide training on student privacy laws to employees with access to an education record. The LEA needs to keep a list of these employees who have completed the training. The employees need to sign a certified statement that they received the training and understand student privacy requirements.

---

**Appendix**

**Data Gateway**

**Using the Data Gateway**

USBE has developed a data entry tool for the Metadata Dictionary in the Data Gateway. To be able to enter data here, you must be given the role of Data Dictionary LEA Editor. In general, the LEA data manager should have this role, though it could also be given to other individuals as needed.

**Accessing the Data Gateway**

To access the tool, you will need to go to the Data Gateway and log in. After logging in, go to [My Tools]. Under the Student Data Privacy heading, you will see [Metadata Dictionary Editor] (see Figure 1). Once inside, you will have two options for entering your information: manual entry and bulk upload.

If you do not see the tool, then you do not have the correct permissions in the Data Gateway and will need to contact the Student Data Privacy Section at USBE to have your permissions updated.

---

**Student Data Privacy Act**

Under this law, LEAs are required to adopt policies to protect student data and designate a data manager. They are also required to create and maintain a data governance plan, a metadata dictionary, and establish an external research review process. LEAs need to classify student data as necessary, optional, and prohibited and notify parents of their data policies. Schools may only collect optional data, such as biometric identifiers, with parental consent. When contracting with a third-party contractor who will use student personally identifiable information, the education entity shall require certain provisions in the contract.

**Student Privacy Act**

The Student Privacy Act requires that LEAs provide training on student privacy laws to employees with access to an education record. The LEA needs to keep a list of these employees who have completed the training. The employees need to sign a certified statement that they received the training and understand student privacy requirements.

---

**Bulk Upload to Metadata Dictionary Tool**

The bulk upload tool is located on the Data Recipients page (see Figure 2). To begin, download the data recipient and data elements templates by clicking on the associated hyperlinks. The first column is titled [ID].

- If you are uploading a new recipient, leave the [ID] field blank.
- If you are modifying an existing recipient, find the Record ID in the recipient list for the record you are modifying (see Figure 3) and enter it into the [ID] field. Note that if you are modifying a record, the vendor name, subtitle, and description fields will not change.
- If you are loading data elements, enter the Record ID on the [Agreement Record ID]. Then mark the data elements you want to add with an “X.”
Lastly, save the template file. Then select [Choose File] (Figure 2) and upload the file. You will get a message confirming all the new rows that have been loaded with the new Record IDs.

• **Federal or state justification:** In the editor, you can use the multi-select box to choose federal, state, local directive, or other for sharing. In the bulk upload template, mark the relevant fields as TRUE and leave the others blank.

• **Justification name:** In the case of federal or state laws, this will be the name of the law, or its section in code. For local directive or other, this could be a memo, board directive, or principal’s decision.

• **URL:** If the justification can be found on another website (e.g., Utah legislature), then a URL can be added that goes directly to the relevant statute.

• **Notes:** You may add additional information regarding the justification here.

### Indicating the Data Elements Being Shared

At the bottom of the page in the manual entry tool, you can locate the data element entry tool by clicking on [Select Data Elements] (Figure 5). The data elements entry list will then open in a new window (Figure 6). Check the boxes for the categories of data that are being shared. Then click [Done] when complete.

### Exporting the Data Dictionary

On the data recipients page, you can download a copy of your data recipient and data elements lists to an Excel file (Figure 4).

In the bulk upload template and the data entry editor, you can use the following fields:

- **McGraw Hill Aleks - Aleks Record ID: 483**
- **Technology Student Association - TSA Record ID: 623**

Figure 3. The Record ID numbers are located to the right of the recipient’s name

Figure 4. Data export tool.

In the bulk upload template and the data entry editor, you can use the following fields:

- **Federal or state justification:** In the editor, you can use the multi-select box to choose federal, state, local directive, or other for sharing. In the bulk upload template, mark the relevant fields as TRUE and leave the others blank.

- **Justification name:** In the case of federal or state laws, this will be the name of the law, or its section in code. For local directive or other, this could be a memo, board directive, or principal’s decision.

- **URL:** If the justification can be found on another website (e.g., Utah legislature), then a URL can be added that goes directly to the relevant statute.

- **Notes:** You may add additional information regarding the justification here.

### Indicating the Data Elements Being Shared

At the bottom of the page in the manual entry tool, you can locate the data element entry tool by clicking on [Select Data Elements] (Figure 5). The data elements entry list will then open in a new window (Figure 6). Check the boxes for the categories of data that are being shared. Then click [Done] when complete.

Figure 5. Data elements entry tool

Figure 6. Data elements entry list
Indicating FERPA Exception
The four most common FERPA Exceptions are listed on the manual entry tool (Figure 7). Additional exceptions are hidden, but can be uncovered by selecting [Show Less Used FERPA Exceptions]. In the bulk entry template, you need to type the name of the exception exactly to match; otherwise, the upload will fail.

Posting a Link to the Metadata Dictionary
The Student Data Protection Act states that each LEA is required to display their metadata dictionary on their website. To do this, simply provide a link to the dictionary. While on the Districts screen, you will see a hyperlink titled “Public Link.” When you click on it, it will take you to your LEA’s specific metadata dictionary. You can then copy the URL in the search bar and post it to your page (see Figure 8).