Kentucky Department of Education

District Guidance: Student Information Security & Privacy

Overview

Recent advances in technology and our ability to use student data to inform instruction and practice have created both unprecedented opportunities and unique challenges for educators. This guidance is intended to assist districts involved in building and using education data systems to develop policies related to data privacy, confidentiality, and security practices. It also includes specific information to guide districts in developing contractual agreements with data integration and data sharing vendors.

General Resources

In an effort to best secure its information systems and protect the privacy of the data that it collects, uses, shares and stores. KDE frequently reviews and updates its practices. The department's Data Access Policy, along with several other guiding documents, is located at the Data Collection/Use webpage.

The U.S. Department of Education's Family Policy Compliance Office oversees implementation of both the Family Education rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA). Both of these laws are aimed at protecting student and parent rights in education. The Family Policy Compliance Office's webpage includes numerous resources to assist districts in understanding the requirements of both of these laws. The website includes access to the laws and regulations, FAQs, webinars and model notices for districts to send to parents concerning the right to access and amend their students' education records and the right the consent to the disclosure of personally identifiable information.

Additionally, the Privacy Technical Assistance Center (PTAC) has developed a body of best practice resources to help education stakeholders implement sound student longitudinal data systems. The PTAC "toolkit" includes case studies, webinars, checklists and other information related to (1) data sharing, (2) disclosure avoidance, (3) security best practices, (4) data governance, and (5) legal references. Please see: Protecting Student Privacy webpage.

Other resources related to the collection, storage and safeguarding of student and educator information, including those published by Education Privacy Information Center, the Data Quality Campaign, and the Fordham Center on Law and Information Policy, are available at Data Privacy and Security webpage.

Data Retention and Disposition

Districts are strongly encouraged to review and comply with the data retention and disposition schedules outlined by the Kentucky Department of Library and Archives in the Public Schools District Retention Schedule.

Maintaining and Providing Training on Data Security and Privacy Policies

Districts are encouraged to develop internal processes for establishing and maintaining data security and privacy policies. Efforts should be made to monitor changes in state and federal regulations that are related to data collection and reporting and update their internal policies accordingly.

In order to minimize the risk of human error and misuse of information, a range of training opportunities should be provided for all staff on these policies. All new employees and contracted partners should be educated on the policies and continuing employees should participate in annual training, which should be a prerequisite for continued access to student and/or educator data. Additionally, targeted information security training should be provided for specific groups within the district, depending on specific roles and responsibilities.

There are good on-line resources that can supplement district created training. Examples include:

Forum Guide to Data Ethics Online Course
FERPA 101: For Local Education Agencies
FERPA 201: Data Sharing under FERPA

Internal Use of Data

The personally identifiable information from students' education records that a district maintains should not be available to all district employees. Access to this information should be provided only to employees who have a reasonable and appropriate need for access to the information in order to maintain the records or to assist in conducting district evaluation, audit, or compliance functions. Districts are encouraged to designate individuals responsible for monitoring whether data is properly handled from collection to reporting. This committee may assist in identifying the individuals who have a legitimate need for access to data and develop policies concerning the management of the district's data.

Breaches in Security

Districts should establish clear methods for preventing and addressing any breaches in security, as recommended by the Kentucky Department of Education in 2006 (see HB 341: Personal Data Security Study which can be found at the Data Security Best Practice Guidelines webpage. Individuals should be designated for addressing concerns about security breaches and identify appropriate consequences, which may need to include termination of employee or contract. The Kentucky legislature updated KRS 61.932 with House Bill 5 in 2014. This update contains specific requirement for state agencies and public school districts if a breach occurs.

Disclosure of Personally Identifiable Student Data

Districts are encouraged to develop policies for the disclosure of personally identifiable student information that both comply with the Family Educational Rights and Privacy Act (FERPA) and best practices. At a minimum, these policies should adhere to the general restrictions imposed by FERPA. Districts are encouraged to go beyond what is required by federal law, including implementation of best practices, where possible.

FERPA does not permit the disclosure of personally identifiable information from student records unless the disclosure is for one of the limited purposes outlined in 34 CFR § 99.31, including the following.

- Use by School Officials for Legitimate Educational Purpose: Student information may be disclosed to school officials who the district has determined to have legitimate educational interests, so long as reasonable methods are used to ensure that the school officials obtain access to only those education records in which they have legitimate educational interests. Note, this includes when the disclosure is to a contractor, consultant, or other party, provided that the third party (1) performs and institutional service or function for which the district would otherwise use employees; (2) is under the direct control of the district with respect to the use and maintenance

of education records; and (3) is subject to the requirements of FERPA, 34 CFR §99.33(a) governing the use and re-disclosure of personally identifiable information from education records.

- Student Transfer and Enrollment: Student information may be disclosed, subject to the requirements of FERPA 34 CFR §99.34, to officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled so long as the disclosure is for notification of this service through its annual FERPA notification letter.

- Education Studies: Student information may be disclosed to organizations conducting studies for, or on behalf of, the district to: (1) develop, validate, or administer predictive tests: (2) administer student aid programs; or (3) improve instruction. Disclosures for the purpose of such studies must ensure that the study is conducted in a manner that does not permit personal identification of parents and students by individual, other than representatives of the organization that have legitimate interests in the information, the information is destroyed when no longer needed for the purposes for which the study was conducted, and the district enters into a written agreement that meets the requirements outlined below.

- Audits or Evaluation: Student information may be disclosed to authorized representatives in connection with an audit or evaluation of Federal or State supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. Disclosures for the purposes of such audits, evaluations, or compliance activities must ensure that the district uses reasonable methods to ensure that its authorized representative: (1) uses personally identifiable information only to carry out an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements related to these programs; (2) protects the personally identifiable information from further disclosures or other uses, in accordance with FERPA; (3) destroys the personally identifiable information in accordance with FERPA; and (4) the district enters into a written agreement that meets the requirements outlined below.

Data Sharing Agreements

School districts have expressed a specific interest in learning more about best practices related to data sharing agreements and contractual agreements with data integration vendors.

The PTAC "toolkit" includes a summary of requirements for written agreements concerning data sharing under FERPA. The FERPA regulations require local authorities to execute a written agreement if personally identifiable information from student records will be shared for the following purposes:

- Conducting a study on behalf of the local education authority [See 34 CFR and §99.31(a)(6)(iii)(C)] and
- Conducting an audit or evaluation of educational programs [See 34 CFR §99.35 (a)(3)].

PTAC also has developed a checklist that delineates the minimum requirements under the research and the audit or evaluation exceptions, followed by best practice suggestions that my help to further enhance the transparency and effectiveness of the agreements. This resource can be found at the Privacy and Data Sharing webpage.

Finally, PTAC has issued guidance that specifically addresses best practices for protecting student data while using online educational services at the Protecting Student Privacy While Using Online Educational Services webpage.

The guidance below is not only based on these PTAC resources, but also includes input from independent privacy experts and is consistent with KDE's policies for data sharing agreements and contracts at the state level.

Disclosure of Student Data for Online Educational Services

Prior to sharing personally identifiable student information for online educational services like computer software, mobile applications, or web-based tools, districts are encouraged to enter into a written agreement or contract that meets the following requirements:

- Make clear whether the data collection belongs to the school/districts or the provider, describe each party's responsibilities in the event of a data breach (see PTAC's Data Breach Response Checklist), and, when appropriate, establish minimum security controls that must be met and allow for a security audit;

- Be specific about the information the online service provider will collect (e.g., forms, logs, cookies, tracking pixels, etc.);

- Define the specific purposes for which the provider may use student information, and bind the provider to only those approved uses. Specify in the agreement how the district will be exercising "direct control" over the third party provider's use and maintenance of the data. Include data archival and destruction requirements to ensure student information is no longer residing on the provider's systems after the contract period is complete. When appropriate, define what disclosure avoidance procedures must be performed to de-identify student information before the provider may retain it, share it with other parties, or use it for other purposes.

- Specify whether the district and/or parents (or eligible students) will be permitted to access the data (and if so, to which data) and explain the process for obtaining access. This is especially important if the online educational services will be creating new education records that will be maintained by the provider on behalf of the district, as FERPA's requirements regarding parental (or eligible students') access will then apply. To avoid the challenges involved in proper authentication of student's parents by the provider, the district is encouraged to serve as the intermediary for these requests, wherein the parent requests access to any education records created and maintained by the provider directly from the district, and the district then obtains the records from the provider to give back to the parent;

- Establish how long the agreement will be in force, what the procedures will be for modifying the terms of the agreement (mutual consent to any changes is a best practice) and what both parties' responsibilities will be upon termination of the agreement, particularly regarding disposition of student information maintained by the provider; and

- Carefully assess the need for and legality of any indemnification and warranty provisions. Determine whether applicable state law limits the district's ability to indemnify a provider. Analyze whether there should be indemnification provisions in which the provider agrees to indemnify the district, particularly relating to a district's potential liabilities resulting from a provider's failure to comply with applicable federal or state laws. Be specific about what you will require the provider to do in order to comply with applicable state and federal laws, such as KRS 365.734 (HB 232), KRS 61.931, et seq. (HB 5), FERPA, and what the provider agrees to do to remedy a violation of these requirements and compensate the district for damages resulting from the provider's violation.

Disclosure of Student Data for Studies of Behalf of the District

Prior to sharing personally identifiable student information for purposes of educational studies for or on behalf of their district, districts are encouraged to enter into a written agreement or contract that meets the following requirements, which both meet and exceed what is required by applicable state and federal laws, such as KRS 365.734 (HB 232), KRS 61.931, et seq. (HB 5), and FERPA:

- Designates the authorized users or entity to serve as the authorized agent. If any entity is designated within the agreement, the agreement must specify the authorized users directly responsible for managing the data in question;

- Specifies the purpose, scope and duration of the study and the information to be disclosed. This description must include the research methodology and why disclosure of personally identifiable information from education records is necessary to accomplish the research. Note, the district should not disclose all of the personally identifiable information from its education records; rather, it will determine only the specific elements needed and disclose only those;

- Requires the authorized users to use personally identifiable information only to meet the purpose of the disclosure as stated in the written agreement and not for commercial purposes or further disclosure. Approval to use the personally identifiable information from the education records for one study, audit, or evaluation does not confer approval to use it for another;

- Requires the authorized users to conduct the study in a manner that does not permit the personal identification of parents and students by anyone other than the representatives of the organization with legitimate interest. The agreement must require the authorized users or entity to conduct the study so as to not identify students or parents This typically means that the authorized users or entity should allow internal access to personally identifiable information from education records only to individuals with a need to know, and that the authorized users or entity should take steps to maintain the confidentiality of the personally identifiable information at all stages of the study, including within the final report, by using appropriate disclosure avoidance techniques;

- Affirms that the authorized users or entity may only publish results in a way that protects the privacy and confidentiality of the individuals involved. For example, when publishing tables, cell suppression and other methods of disclosure avoidance must be used so that students cannot be identified through small numbers displayed in table cells;

- Requires the authorized users or entity to destroy the personally identifiable information from the education records when the information is no longer needed for the purpose specified and must be clear about how the education records will be destroyed. The agreement must identify a specific time period for destruction based on the facts and circumstances surrounding the disclosure and study. The parties to the written agreement may agree to amend the agreement to extend the time period if needed, but the agreement must include a time limit. The agreement must require the authorized users or entity to provide written confirmation to the district when the education records have been destroyed, per the terms of the agreement.

- Documents appropriate technical, physical, and administrative safeguards to protect personally identifiable student data at rest and in transit. Establishes policies and procedures to protect personally identifiable student information from further disclosure and unauthorized use, including limiting use of personally identifiable information to only the authorized users or entity with a legitimate interests in the research or study; and

- Includes a plan for how to respond to any breach in security, including the requirements that any breach in security must be reported immediately to the district. KRS 61.931, et seq. (HB 5) provides specific guidance on data breach notification.

Disclosure of Student Data for Audits, Evaluation or Compliance Monitoring

Written agreements for audits, evaluation or compliance monitoring should be similar to, but slightly different than, agreements for research and studies. These written agreements or contracts should include the following requirements, which both meet and exceed what is required by FERPA:

- Designates the individual that will serve as the authorized representative. The agreement must specify the individuals directly responsible for managing the data in question;

- Specifies the purpose for which the personally identifiable student information from education records is being disclosed and state specifically that the disclosure is in furtherance of an audit, evaluation, or enforcement or compliance activity. The agreement must specify the student information to be disclosed and must include a description of how the student data will be used. The agreement must describe the methodology and why disclosure of personally identifiable student information is necessary to carry out the audit, evaluation, or enforcement or compliance activity;

- Requires the authorized representative to use personally identifiable information only to meet the purpose of the disclosure as stated in the written agreement and not for commercial purposes or further disclosure.

- Requires the authorized representative to destroy the personally identifiable information from the education records when the information is no longer needed for the purpose specified and must be clear about how the education records will be destroyed. The agreement must identify a specific time period for destruction based on the facts and circumstances surrounding the disclosure and study. The parties to the written agreement may agree to amend the agreement to extend the time period if needed, but the agreement must include a time limit. The agreement must require the authorized representative to provide written confirmation to the district when the education records have been destroyed, per the terms of the agreement;

- Documents appropriate technical, physical, and administrative safeguards to protect personally identifiable student data at rest and in transit. Examples of this include secure-file transfer protocols ("SFTP") and hyper-text transfer protocol over secure socket layer (HTTPS"). The agreement must establish policies and procedures to protect personally identifiable student information from further disclosure and unauthorized use, including limiting use of personally identifiable information to only the authorized representatives with a legitimate interest in the audit, evaluation, or enforcement or compliance activity; and

- Includes a plan for how to respond to any breach in security, including the requirement that any breach in security must be reported immediately to the district. For example, at KDE the process would involve reporting the incident to the department's Chief Information Officer. If the Chief Information Officer, in collaboration with the commissioner and appropriate members of the department's executive team, determine that one or more employees or contract partners have substantially failed to comply with the department's information security and privacy policies, they will identify appropriate consequences, which may include termination of employment or a contract and further legal action.

Monitoring Implementation of Data Sharing Agreements

In addition to all of the precautions addressed above, any third party data sharing agreement or contract should, at a minimum, also address the following assurances to protect personally identifiable information from further disclosure and unauthorized use:

- Districts should verify that the authorized representative has a sound data security program to protect data at rest and in transmission. This may be addressed through language in the data sharing agreement that states what data security provisions are required, including requirements related to encryption, where the data can be hosted, transmission methodologies, and provisions to prevent unauthorized access. Districts may wish to require the authorized representative to provide a certification indicating that an independent vulnerability or risk assessment of this data security program has occurred. The district also may wish to maintain the right for the district to physically inspect the authorized representative's premises or technology used to transmit or maintain data;

- Districts should verify that the authorized representative has in place a data governance plan with support and participation from across the organization. A data governance plan is one that details the organization's policies and procedures to protect privacy and data security, including the ongoing management of data collection, processing, storage, maintenance, use and destruction. The district may also wish to verify that the authorized representative has a training program to teach its employees about FERPA and how to protect personally identifiable information from education records.

- If applicable, districts should verify that the authorized representative has appropriate disciplinary policies for employees that violate FERPA, including termination in appropriate instances;

- Districts should maintain the right to conduct audits or other monitoring activities of the authorized representative's data stewardship policies, procedures, and systems. If, through these monitoring activities , a vulnerability is found, the data requestor must take timely appropriate action to correct or mitigate any weakness discovered; and

- Districts should maintain the right to review any data prior to publication and to verify that proper disclosure avoidance techniques have been used to approve reports prior to publication to ensure they reflect the original intent of the agreement.

Consequences for Failure to Comply with Data Sharing Agreements

Districts are encouraged to identify specific consequences for breaches in data sharing agreements or contracts. In addition to developing methods for individuals to report concerns about breaches in security, a policy should be developed for determining whether a breach has occurred and how to respond with consequence. As required by FERPA, if an authorized representative that receives data to perform evaluations, audits, or compliance activities improperly discloses the data, the district must deny that representative further access to personally identifiable data for at least five years. In addition, the district may pursue penalties permitted under state contract law, such as liquidate damages.

Parent Notification about and Access to Student Records

FERPA requires districts to annually notify parents of their rights to:

- Inspect and review their student's education records;
- Seek amendment of the student's education records that the parent believes to be inaccurate, misleading or otherwise in violation of the student's privacy rights;
- Consent to disclosure of personally identifiable information contained in the student's education records (except to the extent that FERPA authorizes disclosure without consent, under section 99.31); and
- File a complaint with the U.S. Department of Education concerning any alleged failures by the district to comply with the requirements of FERPA.

This notice must include specific information about the procedure for exercising the right to inspect and review education records and the procedure for requesting an amendment of records. If the district has a policy of disclosing education records without prior consent to school districts with a legitimate education interest (as permitted by FERPA), the district must specify the criteria it uses for determining who constitutes a school official and what constitutes a legitimate educational interest.

In addition, as required, a school or district employee must obtain a parent's written consent before requiring a student to participate in any survey, assessment, analysis, or evaluation intended to reveal information concerning the student or the student's family, sexual behavior and attitudes, illegal, anti-social, self-incriminating, or demeaning behavior,

critical appraisals of individuals with whom a student has close family relationships, legally recognized privileged or analogous relationships, income (except as required by law), social security number or religious practices, affiliations, or beliefs.

As required, if a district sends a form to a parent requesting written consent for the district to release personally identifiable information concerning the parent's child in education records other than directory information, such consent shall be valid only if the form contains notice to the parent regarding the specific records to be released, the specific identity of any person, agency or organization requesting such information and the intended uses of the information, the method of manner by which the records will be released, and the right to review or to receive a copy of the relevant records to be released.

At the beginning of each school year, each district must provide written notice of a student's rights with respect to federal and state law, as described above.

In addition to what is required by federal and state law, districts are encouraged to carefully consider whether it would like to provide parents and students with any opportunities to opt in or out of other data collections and recordkeeping.