Data Management Best Practices (*5/16/2022)*

Status	Mandatory Requirements	Law/ Regulation
☐	Protection of Pupil Rights Amendment (PPRA) Policy	PPRA - 20 U.S.C. § 1232h; 34 CFR Part 98
☐	Annual Notification - Family Education Rights & Privacy (FERPA) requires a school to annually notify parents of their rights under FERPA (Model FERPA Notification)	34 CFR Part 99.7
☐	Annual Directory Information notice (Model Directory Information Notification)	§ 9528 of the ESEA, 34 CHR 99.37
☐	Annual Notification of Protection of Pupil Rights Amendment (PPRA) --. (Model PPRA Notification) , (PPRA Model Notice & Consent Opt-Out for Specific Activities)	20 U.S.C. § 1232h; 34 CFR Part 98 20 USC 7908
☐	Annual Military Recruiter notification – (Notification is often included in the annual FERPA Notification.)	§ 8528 of the ESEA
☐	Notification to parents that education records are forwarded to other agencies or institutions that have requested the records and in which the student seeks or intends to enroll or is already enrolled as long as the disclosure is for the purposes related to the student's enrollment or transfer. This notice is usually included in the annual FERPA notification.	34 CFR 99.34

Status	Other Best Practices	Law/Regulation
☐	Establish and/or complete an annual review of policies, procedures and/or guidelines around; • Data Governance policy and/or Data Collection, Access & Use • Data Security • Data Breach • Limited Directory Use Policies • Data Retention • Data Destruction • Acceptable Use Policies – data and internet use	
☐	New Employee awareness - set clear expectations for data security and privacy with all new employees a part of orientation. Review district policies, annual notifications and obtain signatures to confirm understanding as applicable. On-line training tools to help with training: • Forum Guide to Data Ethics Online Course • FERPA 101: For Local Education Agencies • FERPA 201: Data Sharing under FERPA	
☐	Annual training plan – reminders for all staff – utilize KDE webpage for resources that can be used.	
☐	Internal data access process: • Establish internal data request process with approvals to confirm "need to know" before granting system access. • Confirm signed acceptable use policy and non-disclosure documents on file before granting access.	

Data Management Best Practices (*5/16/2022*)

Status	Other Best Practices	Law/Regulation
	• Promote best practices on creating and maintaining secure passwords. • Establish/follow notification procedures for when an employee leaves so access can be revoked.	
☐	External data request process to include: • Procedures for internal review – individual or team with understanding of annual notifications and FERPA exceptions • MOUs are executed prior to sharing personally identifiable information. • Parent and Eligible Student Rights – ensure established process is followed to accommodate parent and eligible student rights to access, seek to amend, and consent to disclose data. • Data sharing tracking – maintain documentation of any personally identifiable data that is disclosed.	34 CFR 99, Subparts B,C, and D 34 CFR 99, Subpart D
☐	Data Sharing Agreements • Maintain a written agreement/memorandum of understanding (MOU) for data sharing under FERPA for studies and audit-evaluation exceptions. Although not required, agreements are also a best practice for data sharing under the "officials" exception too. Include KRS 61.931 and KRS 365.734 language. • Ensure data sharing agreements are in place for each data system used. Determine applicable FERPA condition for sharing PII – directory, official, studies, or audit-evaluation. Define purpose, limit use to educational purpose, address security of records, and identify how records will be destroyed. • Reviews opt in agreements to ensure all systems represented.	
☐	Data Inventory • Data collection – Ensure that data are collected in accordance with your collection and survey notices. • Keep accurate and updated data inventories or data dictionary – review/update your metadata dictionary.	
☐	Security Protocols • Implement the Center for Internet Security (CIS) controls for effective cyber defense or a comparable IT security framework • Data Security Checklist for developing/maintaining successful data security program.	

☐	System inventory
	• Identify and maintain inventory of systems used within school and district including apps used in the classroom
	• Establish district or school review/approval process prior to purchase/use to ensure terms of agreement (including on-line apps) are acceptable to school and district and meet FERPA and PPRA requirements.
	• Require service providers and educational partners who handle personal information on behalf of your organization to follow your security policies and procedures as well as state and federal laws. KDE has developed the following verbiage, which, if used by any district, must be customized, for inclusion in contracts:
	  • KDE RFP/Contract Attachment - Data Security and Breach Protocols
	  • KDE RFP/Contract Attachment - FERPA and Affidavit of Non-Disclosure	

☐	Establish and follow data breach best practices for escalation and notification of any issue:	

Data Management Best Practices (*5/16/2022)*

Status	Other Best Practices	Law/Regulation
	• Investigate any incidents to determine if they are data breaches. • Notify KDE of suspected or confirmed breach to ensure state notification procedures are followed. • Ensure that parents, eligible students and faculty as applicable are notified of any data breaches.	

☐	Data Governance
	• Designate individuals to be responsible for:
	  ○ Monitoring whether data is properly handled from collection to reporting
	  ○ Identifying individuals who have legitimate need for access to data
	  ○ Approving outside requests for data
	• Develop polices concerning the management of the district's data.
	• Establish data stewards to monitor and validate quality data.
	• Maintain data calendar with clear expectations for data quality validation.	

☐	Transparency – make data management practices public or readily available: • Maintain inventory of systems and apps used with overview of what's included and how each are used. • Document data sharing agreements in place under FERPA exceptions. • Post annual notices and data management policies on-line on school/district website.	
☐	Other optional notifications can include: • What information is being collected about students; • Why information is being collected; • How information is being protected; • What information is shared with third parties; • Who parents should contact if they have questions about data practices	

Helpful websites:

- Kentucky Department of Education – Privacy and Security webpages - https://education.ky.gov/districts/tech/pages/data-security-privacy.aspx
- U.S. Department of Education – Privacy Technical Assistance Center - https://studentprivacy.ed.gov/
- Student Privacy Resource Center **-** https://studentprivacycompass.org
- Future of Education Privacy Forum - https://fpf.org/2019/04/05/future-of-privacy-forum-releases-policymakers-guide-to-student-data-privacy/