Warren County Public Schools

Data Management Procedures Guide

District Data Management
Procedures Guide

Section 1: Introduction and Overview:

Warren County Public School information (hereafter data) must be managed, used, and protected in accordance with federal and state law as well as school district policies so as to ensure its integrity, availability, privacy, and confidentiality. Each employee, agent, or affiliate of Warren County schools, who handles data for the purpose of performing his/her job duties, or other functions directly related to his or her contractual affiliation with the district, is a steward of data and responsible for the proper handling of data resources under his/her control. Some examples of types of data are payroll, personnel, faculty, student (FERPA/HIPAA), development, financial (school/district), facilities-related, all types of personally identifiable information (PII), and any other data used in the district. Some examples of PII are a child's full name, social security number, physical home address, parent/guardian information, and other such information that can be found on medical records, ILP's, and/or Infinite Campus reports. Some data elements are unique and may have additional protocols for their management and use. These unique data types include, but may not be limited to, survey, marketing, and outsourced data.

It is the obligation of all employees to protect the security and integrity of all data under their control. To reduce the risk of data loss due to devices being lost or stolen, no data should be copied to or stored on portable computing devices (laptops, mobile devices, iPads, ChromeBooks, portable USB drives, etc.). All data should remain on district-owned local network servers, desktop computers, and resources. Resources includes paper, electronic formats/media stored locally within a district owned facility as well as on any/all district owned cloud-based collaboration sites. The District discourages the use of non-organizationally owned cloud-based storage and collaboration services for all types of data. Data containing PII, FERPA, or HIPPA controlled information shall not be stored on any non-organization owned cloud based collaboration site.

Data elements that contains PII are not allowed to be removed from District property whether in a physical or electronic format without written permission. Personally owned devices shall not be used to store or transport data containing PII at any time. Permission to carry physical or electronic copies of specific data containing PII off

campus may be requested in writing from the building level administrator/supervisor. (See Section 4 - Forms) The requesting employee must specify the content and specific use of the data as well as the length of time the data is anticipated to be needed off site. For employees whose job duties involve substantial (amount, length of time, or risk) off site access to PII, a device with additional data safety encryption may be required. Individuals and corporations with contractual obligations which involve access to PII should maintain the security of the data in accordance with all established state and federal regulations.

Violations of this policy/procedure include, but are not limited to: accessing data to which the individual has no legitimate right; enabling (intentional or unintentional) unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedure, or other relevant regulations or laws; inappropriately altering, damaging, or destroying data; inadequately protecting restricted data; or ignoring the explicit requirements for the proper management, use, and protection of data resources. Violations may result in network access revocation, data access revocation, corrective action, and/or civil or criminal prosecution. Violators may also be subject to disciplinary action up to and including dismissal, pursuant to district policies.

If at any time it is suspected that data had been compromised, it is the responsibility of the employee to immediately notify his/her building level administrator/supervisor. It will be the responsibility of the building level administrator/supervisor to immediately notify the Superintendent (or designee) of the data compromise. Pursuant to KRS 61.931 (et. seq.), the District must notify the Kentucky Department of Education (KDE) of any suspected breach in data security. Section 3 outlines additional steps that may be applicable in the event of a suspected or confirmed data breach.

Technology advances (VPN, TeamViewer, PC Anywhere, etc.) allow school personnel the ability to access local district electronically stored data from outside the normal school setting. School personnel who may be granted remote access to the data include: principals, assistant principals, guidance counselors, district level employees, and other personnel as designated by the Superintendent. Before such outside access is granted, the building level administrator/employee supervisor must submit a request for this type of access to the Director of Technology. (See Section 4 - Forms) The employee, agent, or affiliate of Warren County schools assumes full responsibility for maintaining strict confidentiality of the data and must notify the building level administrator/supervisor immediately of any suspected breach of the data.

Section 2 of this document provides the District's Data Management Best Practices (DMBP) for managing access to data and PII. No technological solution or district policy/procedure can promise complete data security, however, the goal of all DMBP statements is to limit the risk associated with any type of data breach or misuse. In all cases, there must be a balance between convenient data access for employees to successfully complete assigned tasks and protecting the data from misuse. In cases where employees are not granted the level of access to data that they feel is necessary to adequately complete their assigned job duties, an appeal to the Superintendent shall be allowed. Pursuant to 702 KAR 1:170, Section 2 will be updated and amended periodically to comply with the latest guidelines from KDE.

By September 30 of each year, The Director of Technology shall acknowledge to the board of education in a public meeting that the district has reviewed the most recent guidance on best practices for personal information security, and implemented the best practices that meet the needs of personal information security in that district.

Section 2: Data Management Best Practices

The District Data Management Best Practices (DMBP) are designed to comply with the following KDE directives and regulations:

- KDE, “Data Security and Breach Notification Best Practice Guide”, V.2.1 April 2015
- KDE, “Data Access Policy”, Policy 003, January 1, 2012
- 702 KAR 1:170. “School district data security and breach procedures”, Draft April 20, 2015
- Office of Education Technology (OET), “Security Best Practices Guideline for Districts”, Version 1.0 – 0000 – January 12, 2010

The DMBP items are subject to change with limited notice to reflect advances in technical capacities as well as changes issued by KDE to the guiding documents. Implementation of the DMBP statements is contingent on adequate school/district staffing and available financial resources. Implementation priorities will be balanced based on the potential risk for data loss and misuse associated with each specific item.

DMBP Statements:

- Offices, classrooms, and computer labs must be secure before leaving it unattended. Students should never be permitted to use computer lab spaces without employee supervision present in the room.
- Logout of the computer, application, Infinite Campus, Office 365 and/or cloud-based collaboration sites when required tasks have been completed or when leaving the computer/device unattended for an extended period of time (Lunch, Pep rallies,meetings, etc.)
- Shutdown computer at the end of the work day.
- Presenters and invited guests to the school/district are welcome to use personally owned equipment upon approval of building administration. District owned devices will be used under the supervision of the building administrator.
- Clearly identify levels of authority and chain of command related to PII.
- Limit printing of documents containing PII in terms of locations and number of copies.
- Shred all physical copies of documents containing PII prior to discarding them.

- Laptops and external storage (i.e. flash drives and external hard drives) containing PII may not leave District property without prior written approval from Building administrator/supervisor.
- PII that is taken off campus in electronic format should be encrypted.
- Employees should regularly backup files that are job critical to their work assignment(s). Any PII included in backup may not be transported off campus.
- Keep PII off personally owned devices.
- Eliminate sending student PII through email, either in text or as an attachment.
- Remote/off site access to data is restricted to those individuals whom the District has an approved Request for Remote Access to Local Server Stored Data on file. Access may not be shared with any other employee or individual.
- No student will be permitted to access FERPA/HIPAA protected data.
- A District password policy that complies with the current KDE guidelines will be maintained. Employees are encouraged to implement “strong” passwords (including varied case, alphanumeric, and special symbols) for any/all systems that they access.
- Passwords are not to be shared between users.
- “Remember Me,” “Remember my Password”, and other automatic logins to websites containing district data (Infinite Campus, CIITS, Office365, Scholastic, Lexia, Dreambox, etc.) should not be enabled.
- Computers should have a screensaver set to lock the computer once activated. Passwords should be required to unlock the screensaver feature.
- Personally owned mobile devices that are used to access employee email should be set to a locked state which requires a passcode to override/access the device.
- Computer administrator (admin) permissions should be limited to identified technical staff, including district Technology Office staff and school technology coordinators (STC).
- Software and computer OS must be kept up to date. Manual updates will be conducted by individuals with admin permissions. Windows OS updates are deployed on a regular basis from the KDE managed Windows Software Update Server system.
- Mobile device apps currently installed on District owned devices should be reviewed to determine if the publisher complies with WCPS’s DMBP and all state guidelines.

- All software and mobile device apps on District owned devices should be vetted by district Technology Office staff prior to install. A request form must be submitted to the Technology Office to begin the review and approval process. (See Section 4 - Forms) KDE and WCPS has a considerable list of preapproved apps that can be installed at any time.
- Access to security camera files, including but not limited to facility and bus footage, will be restricted to a limited number of building administrators and the Technology Office staff. Security video images may be released to law enforcement only after review by the Board of Education Attorney.
- For staff members granted multiple levels (user, administrator, superuser, etc) of access to data systems, practice the principle of least privilege, only login with admin level access if there is an administrative function that needs to be completed and immediately log off when the task is completed.
- Share data only when there is a specific need and for as limited a time as possible. Additional Non-Disclosure agreements may be required for certain data elements.
- Family members of an employee are not permitted to use district owned devices assigned specifically to that individual.
- Staff should add a statement of confidentiality below their email signature line to accompany all outgoing messages.
- Eliminate personally owned Windows devices from the district network.
- Generic logins for students and staff shall be kept to a minimum. Exclusions include Pre-school, Kindergarten, Guest Teachers, and for online testing.
- Create a school/district data security team.
- Foster a culture of data security thoughtfulness.
- Conduct an annual review of all network security procedures and the DMBP guidelines.
- Monthly review of server and shared folders to ensure only authorized users can access the data will be conducted by Technology Office Staff.
- Annual refresher training for all employees on the SafeSchool (or other approved district training website/process) covering technology related procedures and data security will be required.
- There will be a review of AD group memberships on a routine basis by the Technology Office Staff.

- Regularly review school website teacher portals for violations of data security.
- All financial records should comply with all current Payment Card Industry Data Security Standards.
- Post a summary of district's privacy policy, FERPA, HIPAA, and COPA in various locations, including on the district website.
- Unannounced data security audits may be conducted at any time.
- All obsolete hardware slated for disposal should be sanitized either before disposal or by the recycling agent in accordance with the established district/state contract guidelines.
- All records, physical and electronic, must be retained and secured pursuant to 20 USC Section 1232g et seq. & KRS 160.700 et seq, and as reduced in the Kentucky Department of Libraries and Archives Public School District Records Retention Schedule. Training of staff will be overseen by the District Records Retention Officer.

Section 3: Data Breach Procedures

The following is the data breach procedure mandated by KDE. (cf. "Data Security and Breach Notification Best Practice Guide", V2.1 April 2015)

Data Breach Act "Have to" Section

Please be advised that this is a summary. A thorough understanding of KRS 61.931, et seq. (HB 5), along with its included definitions, will be very helpful and is recommended.

- Procedures and practices to safeguard against security breaches must be implemented by any entity that maintains or possesses personal information in accordance with applicable KRS and federal laws.
- For any contracts involving personal information that are entered into or amended after January 1, 2015, specific language requiring protection of the data must be included.

Within 72 Hours of Suspected or Confirmed Breach

1. Begin conducting a “reasonable and prompt” investigation to determine “whether the security breach has resulted in or is likely to result in the misuse of personal information.” Final determination will be made by the Superintendent.

2. Send notification, via the FAC-001 form, to the appropriate agency contacts. If there is an ongoing investigation involving law enforcement which prevents information from being disclosed, use the FAC-002 form. Agency Data Breach Contacts (last updated April, 2015). (Attachment A - Forms)

Within 48 Hours of Completion of the Investigation

Notify the above staff contacts if the investigation finds that the misuse of personal information has occurred or is likely to occur. The length of the investigation is not set, and may vary depending on the complexity of the breach event.

Within 35 Days of Suspected or Confirmed Breach

- Notify all individuals impacted by the breach in a manner required by KRS 61.931, et seq. including information required by the Act. If breach impacts more than 1,000 individuals, nationwide consumer reporting agencies must also be notified.

- If the investigation determines that misuse of personal information has not occurred or is not likely to occur, notification of the impacted individuals is not required, but records of the decision and evidence must be kept. Notification of the agency contacts, above, is still required noting that misuse of personal information has NOT occurred.

Section 4: Data Management Procedure Forms

Request for Mobile App/Software Review and Approval

Request for Remote Access to Local Server Stored Data

Permission to Carry Specific Data Containing PII Off Campus

FAC-001 - Determined Breach Notification Form

FAC-002 - Delay Notification Record

Employee or Contractor General Affidavit of Nondisclosure

District Data Security Team Members

Request for Mobile App/Software Review and Approval

Your signature on the request form below indicates that as the person granted permission to install a mobile app on District owned devices you are solely responsible for keeping any data secure as outlined in this board policy and associated district approved procedures.

Your Name	
School/Department	
Name of App	
Name of Developer	
Description of App and How it increases instructional value	
Price of App	
Will this app be used on multiple devices?	

Signature of Head Building Administrator / Supervisor Date

Signature of Employee Requesting Data Access Date

Director of Technology Date

Approved / Denied

Request for Remote Access to Local Server Stored Data

Your signature on the request form below indicates that as the person granted data access you are solely responsible for keeping the data secure as outlined in this board policy and associated district approved procedures.

_____ is hereby requesting that _____
(Building Administrator/Supervisor) (Employee Name)
be granted access to data from outside the normal work setting. I have read the above policy and agree to protect data as outlined in the above policy.

_____

Signature of Head Building Administrator / Supervisor Date

_____

Signature of Employee Requesting Data Access Date

_____

Superintendent/Designee Date

Permission to Carry Specific Data Containing PII Off Campus

Your signature on the request form below indicates that as the person granted data access you are solely responsible for keeping the data secure as outlined in this board policy and associated district approved procedures.

_____ is hereby requesting permission to carry specific
(Employee Name)
Personally Identifiable Information (PII) off campus for the following instructional reason:

_____
_____
_____
_____
_____

Data Format: USB/portable storage device ----- laptop ----- paper
Circle all that apply

The PII will be returned no later than _____
(mm/dd/yyyy)
I have read the Data Management Policy and agree to protect data as outlined in the policy.

_____
Signature of Head Building Administrator / Supervisor Date

_____
Signature of Employee Requesting Data Access Date

Determined Breach Notification Form

Section 1

Complete and submit within 72 hours of determination or notification.

Determine:

- ❏ Finance Cabinet Secretary
- ❏ Auditor of Public Accounts (APA)
- ❏ Kentucky State Police (KSP)
- ❏ Attorney General (AG)
- ❏ Commissioner of Department of Library and Archives, if breach determined
- ❏ Chief Information Officer of Commonwealth Office of Technology
- ❏ If Department of Local Government under KRS 61.931(1)(b) or (c) also contact:
- ❏ Commissioner of Department of Local Government
- ❏ If Public School District listed in KRS 61.931(1)(d) also contact:
- ❏ Commissioner of Kentucky Department of Education
- ❏ If Educational entity listed under KRS 61.931(1)(e) also contact:
- ❏ President of Council on Postsecondary Education

Agency Name:	Warren County Public Schools		
Agency Contact:	Rob Clayton		
Agency Contact Email:	rob.clayton@warren.kyschools.us		
Agency Contact Phone Number:	270-781-5150		
Date of Notification to Agencies:		Time of Notification:	
Date Breach Determined:			

Determined Breach Notification Form

Section 2

Complete this portion after the conclusion of the investigation regarding whether the Security Breach has resulted in or is likely to result in the misuse of personal information. Provide notice to agencies within 48 hours of completing investigation.

Personal Information Breached:	▢ Yes ▢No				
	If Yes, Explain:				
	Total Number of Individuals Impacted:		Date Individuals Notified:		
	Type of Notices Sent Out (select all that apply and provide explanations):				
	▢ Web Posting:		▢ Email:		
	▢ Local or Regional Media:		▢ Telephone:		
	▢ Letter:		▢ Other:		
Did You Notify Consumer Credit Reporting Agencies?	▢ Yes ▢No		If Yes, Date:		
Any Other Breach Compliance Requirements Apply such as Federal?	▢ Yes ▢No				
	If Yes, Explain:				

Third Party Breach: ▢ Yes ▢No

If Yes, Name of Third Party: _____

If Third Party Involved, When Did They Notify the Agency: _____

If a delay then please attach the delay notification record along with supporting documentation. Was there a delay due to:

- Law enforcement investigation. Reference to KRS 61.933 (3)(a)
- An agency determines that measures necessary to restore the reasonable integrity of the data system cannot be implemented within the timeframe established and will delay the breach determination. Delay will need to be approved in writing from the Office of the Attorney General. Reference to KRS 61.933 (3)(b)

Determined Breach Notification Form
Section 3
Complete and submit at the conclusion of the investigation and any notice and resolution process.

Actions Taken to Resolve Breach:

_____

Actions Taken to Prevent Additional Security Breaches in Future, if any:

_____

A General Description of what Actions are Taken as a Matter of Course to Protect Personal Data from Security Breaches:

Any Quantifiable Financial Impact to the Agency Reporting the Security Breach:

Reference:
KRS 61.931 to 61.934 - http://www.lrc.ky.gov/Statutes/statute.aspx?id=43575
KRS 42.726 - http://www.lrc.ky.gov/Statutes/statute.aspx?id=43580

Delay Notification Record

All documentation in reference to the delay should be attached to the notification record.

Agency Name: **Warren County Public Schools** _____

3rd Party Name, if applicable: _____

Agencies are to use this form to record information:

- If a law enforcement investigation has delayed the notification process for a breach determination. Reference to KRS 61.933 (3)(a)

Date Law Enforcement Notified Agency: _____

Law Enforcement Agency: _____

If an agency determines that measures necessary to restore the reasonable integrity of the data system cannot be implemented within the timeframe established and will delay the breach determination. Delay will need to be approved in writing from the Office of the Attorney General. Reference to KRS 61.933 (3)(b)

Date Submitted to Office of Attorney General:_____

Date Approved by the Office of Attorney General:_____

The agency will submit form FAC-001 as required by KRS 61.933 if law enforcement has not contacted it within seventy-two (72) hours of a determined breach.

Warren County Public Schools

GENERAL AFFIDAVIT OF NONDISCLOSURE

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT

If during the course of this agreement, Warren County Public Schools, hereafter known as DISTRICT, discloses to the contractor any data protected by the Family Educational Rights and Privacy Act of 1974 (FERPA), as amended, and its regulations, and data protected by the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq)(NSLA) and Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.)(CNA) the contractor is bound by the confidentiality, security and redisclosure requirements and restrictions stated in FERPA, NSLA and CNA and will enter into a confidentiality agreement and ensure its employees and contractors execute affidavits of nondisclosure as required by DISTRICT. The confidentiality agreement and affidavits will then become part of this original agreement.

GENERAL AFFIDAVIT OF NONDISCLOSURE

Name_____

Title_____

Office_____

Supervisor_____

Address _____

Phone_____

If, in the performance of my official job duties, I am provided access to confidential information (information designated as confidential by FERPA, NSLA, CNA, KRS 61.931(6), or other federal or state law), by signing this document I agree to the following:

- I will not permit access to confidential information to persons not authorized by the DISTRICT.
- I will maintain the confidentiality of the data or information.
- I will not access data of persons related or known to me for personal reasons.
- I will not reveal any individually identifiable information furnished, acquired, retrieved, or assembled by me or others for any purpose other than statistical purposes specified in a DISTRICT survey, project, or proposed research.
- I will report, immediately and within twenty-four (24) hours, any known reasonably believed instances of missing data, data that has been inappropriately shared, or data taken off site
    - to my immediate supervisor, and
    - to the DISTRICT Office for whom I perform work under the contract if I am a DISTRICT contractor or an employee of a DISTRICT contractor.

I understand that procedures must be in place for monitoring and protecting confidential information.

- I understand and acknowledge that FERPA-protected information obtained under provisions of Family Educational Rights and Privacy Act of 1974 (FERPA) as an employee or contractor of DISTRICT is confidential information. DISTRICT protects information in students' education records that are maintained by an educational agency or institution or by a party acting for the agency or institution, and includes, but is not limited to the student's name, the name of the student's parent or other family members, the address of the student or student's family, a personal identifier, such as the student's social security number, student number, or biometric record, other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name, and other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

- I understand that any unauthorized disclosure of confidential information is illegal as provided in FERPA and in the implementing of federal regulations found in 34 CFR, Part 99. The penalty for unlawful disclosure is a fine of not more than $250,000 (under 18 U.S.C. 3571) or imprisonment for not more than five years (under 18 U.S.C. 3559), or both.

- I understand and acknowledge that children's free and reduced price meal and free milk eligibility information or information from the family's application for eligibility, obtained under provisions of the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq)(NSLA) or Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.)(CNA) and the regulations implementing these Acts, is confidential information.

- I understand that any unauthorized disclosure of confidential free and reduced price lunch information or information from an application for this benefit is illegal as provided in the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq)(NSLA) or Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.)(CNA) and the regulations implementing these Acts, specifically 7 C.F.R 245.6. The penalty for unlawful disclosure is a fine of not more than $1,000.00 (under 7 C.F.R. 245.6) or imprisonment for up to one year (under 7 C.F.R. 245.6), or both.

- I understand that KRS 61.931 also defines "personal information" to include:

    - an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

    - An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;(b) A Social Security number;

    - A taxpayer identification number that incorporates a Social Security number;

    - A driver's license number, state identification card number, or other individual identification number issued by any agency;

    - A passport number or other identification number issued by the United States government; or

    - Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g.

- I understand that other federal and state privacy laws protect confidential data not otherwise detailed above and I acknowledge my duty to maintain confidentiality of that data as well.

- I understand that any personal characteristics that could make the person's identity traceable, including membership in a group such as ethnicity or program area, are protected.

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

Signature_____

Company/Organization_____

Date_____

District Data Security Team

Kathy Goff, Chief Operations Officer
Jason Kupchella, Chief Academic Officer
Chris McIntyre, Chief Financial Officer
Michelle Blick, Director of Special Education
Michele Tolbert, Director of Human Resources
Pat Stewart, Director of Pupil Personnel
Robert Forsythe, Director of Technology
Ransom Bennett, Computer Technician
Robert Flora, Asst. Director of Technology
Abe Varghese, Computer Technician

Change Control Page

Revision Date	Section & Tile	Page Numbers	Summary of Changes	Author
9/16/15				