

Data Security Annual Report

February 2025

Submitted by

Amy Buss
WCPS Director of Technology

Submitted to

Warren County Public School Board of Education
Garry Chaffin, Chairman
Amy Duvall, Vice Chair
Adam Jackson, Member
Thomas Manco, Member
Jennifer Kash, Member
Robert Clayton, Superintendent

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, ILPs, 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 cloud services such as Google Drive. Resources include 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 HIPAA controlled information shall not be stored on any non-organization owned cloud based collaboration site.

Technology advances (VPN, TeamViewer, Chrome Remote Desktop, 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, 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.

During the 2023-24 school year, the Technology Office staff have continued introducing Amplified IT's recommendations in testable portions to ensure the stability of the network and its access by users. The audit and testing records are available under separate cover and are also marked classified.

The District also conducts regular security assessments.

Warren County Public Schools supports the instructional use of Artificial Intelligence (AI) in the classroom as an accelerator for student learning. WCPS promotes digital literacy and the preparation of students to succeed in postsecondary and/or career opportunities in which there is a growing need for qualified individuals. Integrating artificial intelligence (AI) into K-12 education settings requires meticulous data management and adherence to robust procedures to ensure the technology is both effective and secure. Schools must establish clear policies for data collection, storage, and usage, emphasizing the protection of student privacy in compliance with regulations such as FERPA. It is essential to use AI tools that are transparent in their data processing methods, offering educators and administrators insight into how data is used to inform educational decisions. Regular audits and assessments should be conducted to ensure the AI systems are functioning as intended and free from biases that could impact student learning outcomes. Additionally, educators should be trained in the ethical implications of AI usage and equipped with strategies to integrate these tools seamlessly into the curriculum, fostering an environment where AI enhances learning while maintaining the highest standards of data security and integrity. The United States Department of Education (DOE) has published two documents providing helpful information concerning how AI will affect public education. Additionally, the Kentucky Department of Education has drafted an AI Policy Brief, providing guidance to Kentucky school districts. These documents can be accessed via the following links:

[Artificial Intelligence and the Future of Teaching and Learning](#)

This is the full 73-page report published by the DOE

[Handout: AI and the Future of Teaching and Learning](#)

This is a 4-page synopsis of the full DOE report.

[Kentucky Department of Education AI Policy Brief](#)

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.

Section 3 is the required procedure the District must take in the event of a data breach. This includes both an internal breach as well as an external breach. To date the procedure has not changed.

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. This report serves as the acknowledgement.

Section 2: Data Management Best Practices

The District Data Management Best Practices (DMBP) are designed to comply with the following KDE directives and regulations: Responsibilities for using technology within the District are identified in the Acceptable Use Policy (AUP).

- KDE, "Data Security and Breach Notification Best Practice Guide", V.2.2 September 2015
- KDE, "Data Collection Access and Use Policy", Policy 003, January 1, 2012
- 702 KAR 1:170. "School district data security and breach procedures", Draft April 20, 2015
- KDE, "Data Governance Policy", March 1, 2009
- Office of Education Technology (OET), "Security Best Practices Guideline for Districts", Version 1.0 – 0000 – February 24, 2017

Best Practice	Current Action
Offices, classrooms, and STEM/STEAM labs must be secure before leaving it unattended. Students should never be permitted to use STEM/STEAM lab spaces without employee supervision present in the room.	Self Monitored by Staff responsible for respective office or room
Lock the computer, application, Infinite Campus, GMail, Google Drive, and/or other 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.)	The District, in cooperation with KDE, has instituted a multi-factor authentication requirement for all staff accounts The district has a Chromebook setting for all staff Chromebooks that requires re-authentication after 20 minutes.
Presenters and invited guests to the school/district are welcome to use personally-owned equipment on the public/guest wireless (WCPS_Public) network when granted approval by building or district administration. District	Invited guests use the publicly accessible wifi.

owned devices will be used under the supervision of the building administrator.	
Clearly identify levels of authority and chain of command related to PII. As necessary, building Principals and Central Office Department Directors are responsible for granting access to all data elements under their control.	Access to sensitive information is controlled by least privilege by Network Admins
Limit printing of documents containing PII in terms of locations and number of copies. The product PaperCut should help keep documents containing PII secure until the teacher needs them and not left on the copier unsecured.	The use of Paper Cut has reduced the number of abandoned documents on the Copier/Printers.
Employees should regularly backup files that are job critical to their work assignment(s) to Google Drive. Any PII included in backup may not be transported off campus.	Teachers are responsible for maintaining sensitive documents secure on Google Drive. This includes regular operating system updates.
Keep District PII off personally owned devices.	Self Monitored. Staff are encouraged to use the district supported Google Drive for data storage.
Eliminate sending student PII through email, either in text or as an attachment. Instead share a link in Google Drive or use self-destructing messages in order to maintain encryption security.	Spot checking email indicates a reduction of sending District PII as open text.
Remote/offsite access to local server stored 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. (Section 4: Forms)	Privileged Access Management has been successful to limit the number of remote access users to the District network. EX: HVAC, Finance is moving toward less need for VPN access
No student will be permitted to access FERPA/HIPAA/COPA protected data.	Monitored by Building/Department Administrator

A District password policy that complies with the current KDE guidelines	Self-serve password reset has helped reduce the number of password change requests to unusual circumstances needing Help Desk assistance.
Passwords are not to be shared between users.	It is the responsibility of the staff to keep passwords inaccessible to others.
"Remember Me," "Remember my Password", and other automatic logins to websites containing district data (Infinite Campus, CIITS, GMail, GoogleDrive, Scholastic, Lexia, Dreambox, etc.) should not be enabled.	Self-Monitored. This is not hard and fast "need to", but is recommended if at all possible.
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.	Self-Monitored
Computer administrator (admin) permissions should be limited to district Technology Office staff. Permissions will follow a principle of least privilege.	Permissions are set by the Network Administrators
MDM software and Google Management handle updates and app installs for iPads and Chrome devices respectively. Employees shall apply these updates on site on a regular monthly basis to the devices they are assigned. This includes classroom devices assigned to the students. Some specialized software will have to be manually installed. The process for requesting new software is through the district's technology work order software. It is the responsibility of the user to keep that software up to date. Windows OS updates are deployed on a regular basis from the KDE managed Windows Software Update Server system.	Self-Monitored
All software (instructional and operational) and mobile device apps on District owned devices will be vetted by	The auto-generated list of approved apps has been disabled making it necessary for all requests to go through the

<p>district Technology Office staff prior to installation. An approval request must be submitted to the Technology Office through the district's technology work order system. This requirement also applies to any vendor wishing to do business with the District and will store personally identifiable information (PII) prior to executing any contract with the vendor.</p>	<p>Technology work order system. With the customized format for certain requests, even without the list the process for approval has improved on the individual level. There is still an occasional district wide contract that is submitted late, but it has become more rare.</p>
<p>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.</p>	<p>Monitored by building administrators. In the event of a need to view segments of video, requests will be made to the Technology Office.</p>
<p>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.</p>	<p>Monitored by Network Team</p>
<p>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. Must be approved by the building administrator or supervisor.</p>	<p>Monitored by Building Administrator</p>
<p>Family members of an employee are not permitted to use district owned devices assigned specifically to that individual.</p>	<p>Limited monitoring can be accomplished by the Network Team.</p>
<p>Generic logins for students and staff shall be kept to a minimum. Exclusions may include specific program service accounts and for online testing.</p>	<p>Monitored by Network Team</p>

Update the school/district data security team roster.	Monitored by Tech Team. Members are subject to change each year.
Foster a culture of data security thoughtfulness.	Self-Monitored
Conduct an annual review of all network security procedures and the best practices in Section 2	Accomplished by the Tech Team and reviewed by the data security team.
Monthly review of District server folders to ensure only authorized users can access the data will be conducted by Technology Office Staff.	Monitored by Tech Team Penetration Audits have been completed
Annual refresher training for all employees on the approved district training website/process, covering technology related procedures and data security will be required.	Currently accomplished through district-approved training videos service. One Internet safety/data security video is part of the training videos. The Technology Office has reached out to Human Resources to find other videos.
There will be a review of AD group memberships on a routine basis by the Network Team	On-going
Review school website teacher portals for violations of data security two times per year: fall and spring break.	The Communications Department will review any potential violations and take appropriate action.
This document is available for viewing on the District website.	On-going
Unannounced data security audits may be conducted at any time. These will be conducted by the Network Team.	Self-Monitored
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.	On-going. The vendor has agreed to sanitize all storage hardware prior to disposal
Incident Reports should be used in the event of a possible data breach. Particularly in the event of a lost or stolen	On-going

device. An online incident form is available for Technology Office use.	
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.	On-going. Refer to Becky Hurley, District Archivist. Training - November 1, 2022
Staff should use District owned devices for remote work.	There are security protocols embedded in the District owned devices that have a greater chance of protecting the user's information
Avoid public-use computers.	A general safety practice
Keep data in Google Drive.	District provides Google Drive as the standard data storage application. Any other storage sites are not supported by the Technology Office
Never pick up an unknown USB stick.	Self Monitoring
Never type passwords with "show" activated.	Self Monitored
Keep devices hidden, or better yet, in the trunk of your vehicle.	Self-Monitored
Beware of wifi connections that "look" to be available.	Self Monitored
Due to an increase in data alerts, the technology department will spend more time monitoring and investigating alerts..	Ongoing Tech Team Project. Steps include blocking emails and removing emails before they reach the user
Remote workers should use a good headset with a microphone to prevent others from listening in on conversations.	Self Monitored
Eliminate, as much as possible, background noises such as barking dogs,	Self Monitored

television volume, etc, while on virtual calls (Google Meet, Zoom, Microsoft Teams, etc.)	
Take short breaks throughout the day. This keeps you more alert and aware of potential cyber-threats.	Self Monitored

Section 3: Data Breach Procedures

The following is the data breach procedure mandated by KDE. (cf. "Data Security and Breach Notification Best Practice Guide", V2.2 September 2015)

Data Breach Act

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 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

Information Security Incident Form

Vendor Data Breach Affirmation Template

District Data Security Team Members

Change Control Page

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

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 is 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 the investigation.

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

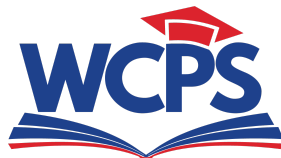
- I understand and acknowledge that FERPA-protected information obtained under provisions of Family Educational Rights and Privacy Act of 1974 (FERPA) as an employee or contractor of DISTRICT is confidential information. DISTRICT protects information in students' education records that are maintained 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_____



Information Security Incident Report Template

REPORTED BY: _____ DATE OF REPORT: _____
 TITLE / ROLE: _____ INCIDENT NO: _____

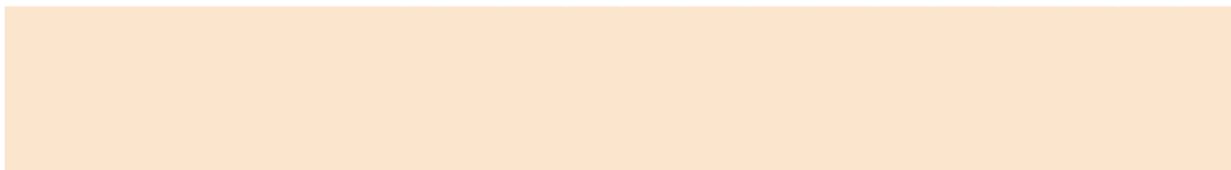
INCIDENT ASSESSMENT _____ NEGLIGIBLE _____ MINOR _____ SIGNIFICANT _____ CRITICAL

SECURITY INCIDENT INFORMATION

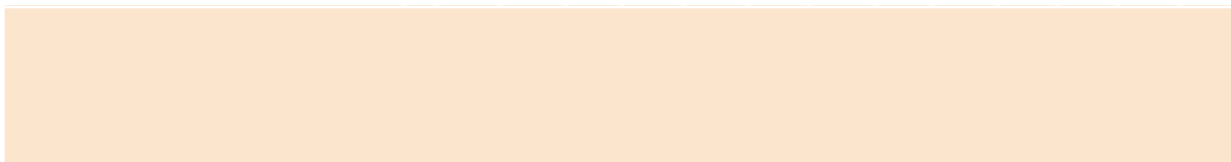
DATE OF INCIDENT: _____ TIME OF INCIDENT: _____
 INCIDENT MANAGER: _____ TITLE / ROLE: _____
 PHONE: _____ EMAIL: _____
 LOCATION: _____
 SPECIFIC AREA OF LOCATION: _____
 INCIDENT TYPE: _____

NO. OF HOSTS AFFECTED: _____ SOURCE IP ADDRESS: _____
 IP ADDRESS: _____ COMPUTER / HOST: _____
 OPERATING SYSTEM: _____ OTHER APPLICATIONS: _____

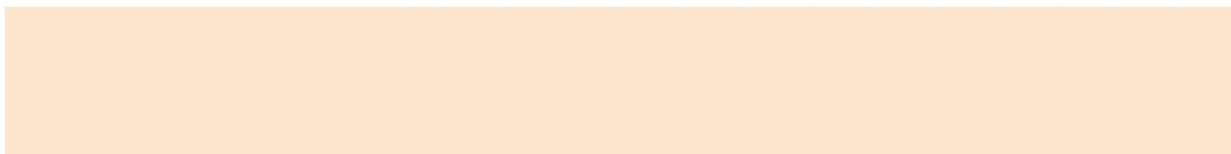
INCIDENT DESCRIPTION:



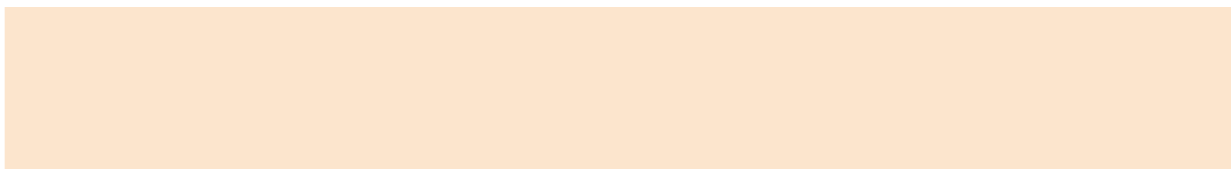
IMPACT ASSESSMENT:



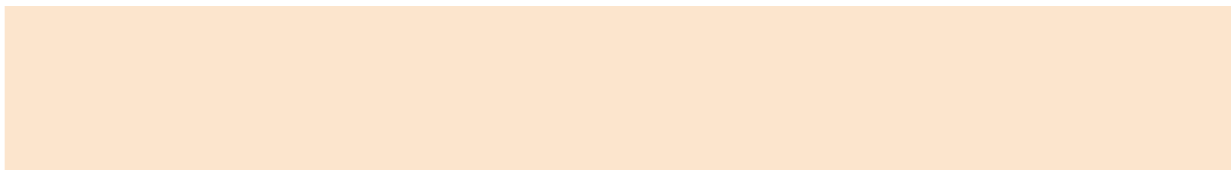
RESULTING DAMAGE:



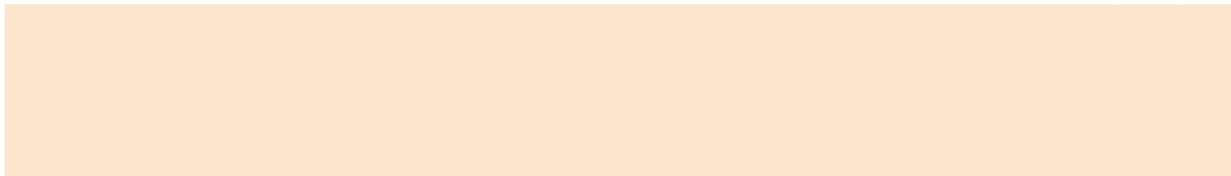
IMMEDIATE ACTION TAKEN:

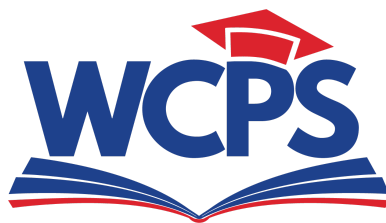


PLANNED ACTION AND RESULTING PREVENTATIVE MEASURES:



ADDITIONAL INFORMATION:





SUBJECT: Affirmation of Data Breach Notification

All software/online instructional vendors wishing to do business with Warren County Public Schools (District) must complete an affirmation of compliance with our data breach notification policy contained in the Warren County Public Schools Data Management Procedures Guide. This affirmation must be submitted on company letterhead and signed by an authorized representative of the company. An email attachment of the affirmation is permissible.

In the event that the vendor does not maintain personally identifiable information about students or staff, then a notification to that effect must be submitted on company letterhead and signed by an authorized representative of the company. An email attachment of the notification is permissible.

Below is a template the vendor may use to submit the affirmation of data breach notification to the District.

(VENDOR) shall report to District any: (1) unauthorized access, use, disclosure, modification, or destruction of Student/Staff Record Information that becomes known to (VENDOR); or (2) interference with (VENDOR'S) information systems operations, of which (VENDOR) becomes aware. (VENDOR) shall notify District of any use or disclosure of Student/Staff Record Information by (VENDOR) not permitted by this Contract, any security incident involving Student/Staff Record Information, and any breach or loss of Student/Staff Record Information, within twenty-four (72) hours.

Legislative authority - KRS 61.931 et. seq.

The affirmation is to be submitted to the Director of Technology or stated designee.

District Data Security Team

Sarah Johnson, Assistant Superintendent

Kyle Cassady, Assistant Superintendent

Chris McIntyre, Chief Financial Officer/Chief Operations Officer

Monica Heavrin, Director of Special Education

Wesley Waddle, Director of Human Resources

Shea Guy, Human Resources Operations Coordinator

Jeff Moore, Director of Pupil Personnel

Kelly Holt, Director of Dining and Nutrition Services

Amy Buss, Director of Technology

Ashley Vincent, District Digital Learning Coach

Dylan Howard, Data Engineer

Lauren Thurmond, Communications Coordinator

Change Control Page

Revision Date	Section & Title	Page Numbers	Summary of Changes	Author
14 July 2016	Section 1	3	September 30 to August 31	JRB
2 August 2017	Committee Members	22	Updated member list	RFF
30 November 2017	Best Practices	5, 6	Added (Section 4: Forms), "has" to have"	JRB
7/6/18	Section 1	2	Added "that involves PII"	JRB
7/6/18	Section 2	4 Point 2 DMBP Statements	Remove Office365	JRB
7/6/18	Section 2	4, Point 4	Change "upon approval of building administration." to " on the public/guest wireless network when granted approval by building or district administration."	JRB
7/11/18	Section 2	4, point 5	Added "As necessary, building Principals and Central Office Department Directors are responsible for granting access to all data elements under their control."	RFF
7/11/18	Section 2	5, Point 14	Added, " for Active Directory services"	RFF
7/11/18	Section 2	5, Point 16	Remove "Office365", add "Gmail, Google Drive"	JRB
7/11/18	Section 2	5, Point 20	Rewritten to reflect the addition of Munki, LightSpeed Management, and Google Admin	JRB

Revision Date	Section & Title	Page Numbers	Summary of Changes	Author
7/11/18	Section 2	6, Point 27	Change from "Staff should add a statement of confidentiality below their email signature line to accompany all outgoing messages." to "If not included automatically by the district email system, employees should use a statement of confidentiality below their email signature line on all outgoing messages."	RFF
7/11/18	Section 4	10	Added to table of contents, "Information Security Incident Form"	JRB
7/29/2019	Section 4	TOC	Added Link to App Approval Form and removed paper form	RCF
7/6/2021	Section 1	2-3	Revision of the section	JRB
7/6/2021	Section 2	4-10	Revision of section created a table BMP and Actions Added NOTE - The Tech Team is currently researching vendors to assist the Tech Team to build a culture of data security awareness. The criteria the Tech Team has established are :...	JRB
7/6/2021	Section 4	27	Removed Michelle Tolbert and replaced with TBD Removed Gina Howard and replaced with Kelly Holt	JRB
7/5/22	Section 2	4	Change "computer" to "STEM/STEAM"	JRB
7/5/22	Section 2	4	Add "WCPS_Public"	JRB
7/5/22	Section 2	5	Add "Occasional network issues have required staff to reset Paper Cut."	JRB

Revision Date	Section & Title	Page Numbers	Summary of Changes	Author
7/5/22	Section 2	5	Add "Obsolete cloud storage, such as DropBox, should be investigated to purge old PII."	JRB
7/5/22	Section 2	5	Add "users"	JRB
7/5/22	Section 2	6	Add "KDE is conducting a feasibility study on implementation of passwordless access."	JRB
7/5/22	Section 2	6	Remove Sec. 2 cell 6L and replace with "LightSpeed Management software and Google Management handle updates and app installs for iPads and Chrome devices respectively. Employees shall apply these updates on site on a regular monthly basis to the devices they are assigned. This includes classroom devices assigned to the students. Some specialized software will have to be manually installed. The process for requesting new software is through the district's Mojo Helpdesk program. It is the responsibility of the user to keep that software up to date. Windows OS updates are deployed on a regular basis from the KDE managed Windows Software Update Server system."	JRB
7/5/22	Section 2	6-7	Remove Section 2, Cell 1L and replace with, "All software and mobile device apps on District owned devices will be vetted by district Technology Office staff prior to installation. An approval request must be submitted to the Technology Office through the district's Mojo helpdesk system."	JRB

Revision Date	Section & Title	Page Numbers	Summary of Changes	Author
			This requirement also applies to any vendor wishing to do business with the District and will store personally identifiable information (PII) prior to executing any contract with the vendor.”	
7/5/22	Section 2	6-7	Replace Section 2, cell 1R with “The auto-generated list of approved apps has been disabled making it necessary for all requests to go through Mojo. With the customized format for certain requests, even without the list the process for approval has improved on the individual level. There is still an occasional district wide contract that is submitted late, but it has become more rare.	JRB
7/5/22	Section 2	7	Change Section 2 cell 3R from “Self Monitored” to “Monitored by Network Team”	JRB
7/5/22	Section 2	7	Change “Tech” to “Network”	JRB
7/5/22	Section 2	7	Change “Network Administrators” to Network Team”	JRB
7/5/22	Section 2	8	Change “Network Administrators” to “Network Team”	JRB
7/5/22	Section 2	8	Replace Section 2 cell 6R with “The Communication Department is in the process of revamping the District Website”	JRB
7/5/22	Section 2	8	Change “Technology Staff” to “Network Team”	JRB
7/5/22	Section 2	9	Replace Section 2, cell 2R with “During the virtual learning event, hotspots were distributed to homes	JRB

Revision Date	Section & Title	Page Numbers	Summary of Changes	Author
			through a point person at each school. These have been returned”	
7/5/22	Section 2	9	Change “hot spots were” to “hotspots are available to be” Remove “These have been returned”	JRB
7/5/22	Section 2	9	Remove “Create business continuity plans for cyber-threats on remote work devices.” Remove “In process”	JRB
7/5/22	Section 2	10	Add “while on Zoom calls or Google Classroom”	JRB
7/5/22	Section 2	8	Change “See Note Below” to “Self-Monitored”	JRB
7/5/22	Section 2	10	Remove “ NOTE... ”	JRB
7/5/22	Section 4	13	Remove “Request for Mobile App/Software Review and Approval (Through our ticketing system)”	JRB
7/5/22	Section 4	27	Remove “Robert Forsythe, Technology Resource Teacher / Data Integration”	JRB
7/5/22	Section 4	27	Add “Data Security Coordinator” Add “Dylan Howard, Data Engineer”	JRB
7/13/22	Section 4	27	Add “Lauren Thurmond, Communications Coordinator”	RFF
7/13/22	Section 4	27	Replace “Michelle Blick” with “Monica Heavrin”	JRB
5/8/23	Title Page	Cover	Remove Confidential watermark	JRB
5/8/23	Title Page	Cover	Update BOE member list	JRB
5/8/23	Title Page	Cover	Change “2022” to “2023”	JRB

