

Request to Place an Item on the Agenda

Name: MATT Laughlin
Address: 285 Airport Rd
Telephone number: 270 265 2436
Name of school children attend, if applicable: District
Group represented: District
Check if request was submitted to: ☒ Superintendent ☒ Board Chairperson
Conferred with following administrators (names): Myself

Description of Issue: Review "Notice of Security Breach & Investigation Procedures"

Specific Action Requested: _____

Check if you are: ☐ Board Member ☒ District Employee ☐ Community Member

All requests for items to be placed on the agenda must be submitted to the Superintendent prior to the Board meeting as specified in Board Policy 01.45. Items submitted shall require prior approval of the Superintendent.

Review/Revised: 3/13/06

Notice of Security Breach & Investigation Procedures**PROTECTION AND PREVENTION**

The District will take reasonable security measures in accordance with KRS 61.931 - KRS 61.933, to guard against the foreseeable loss or exposure of personal information that it maintains or possesses.

“Personal information” is defined as an individual’s first and last name or first initial and last name; personal mark; or unique biometric or genetic print or image, along with any data element listed below:

- Account number, credit or debit card number, that, in combination with any required security code, access code, or password would permit access to an account;
- Social Security number;
- Taxpayer identification number that incorporates a Social Security number;
- Driver’s license number, state identification card number, or other individual identification number issued by any agency;
- 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.

Personal information does not include information that is lawfully made available to the general public pursuant to state or federal law or regulation.

A “security breach” refers to:

- an unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that compromises or is reasonably believed to compromise the security, confidentiality, or integrity of personal information and results in the likelihood of harm to one (1) or more individuals; or
- an unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of encrypted records or data containing personal information along with the confidential process or key to unencrypt the records or data that compromises or is reasonably believed to compromise the security, confidentiality, or integrity of personal information and results in the likelihood of harm to one (1) or more individuals.
- A security breach does not include the good-faith acquisition of personal information by an employee, agent, or nonaffiliated third party of the agency for the purposes of the agency if the personal information is used for a purpose related to the agency and is not disclosed to others without authorization.

INITIAL ASSESSMENT/INVESTIGATION OF SECURITY INCIDENT AND NOTICE

When the District receives information or notice prompting a reasonable belief that an event compromising the security of personal information maintained by the District or nonaffiliated third party on behalf of the District may have occurred, the District shall conduct a reasonable initial assessment or investigation to determine whether the event constitutes a “security breach” under the above definition.

Notice of Security Breach & Investigation Procedures**INITIAL ASSESSMENT/INVESTIGATION OF SECURITY INCIDENT AND NOTICE (CONTINUED)**

Once it is determined that a security breach relating to personal information has occurred, the District shall within seventy-two (72) hours: 1) notify the Commissioner of the Kentucky State Police, the Auditor of Public Accounts, the Kentucky Attorney General and the Education Commissioner and 2) begin a reasonable and prompt investigation to determine whether the security breach has resulted or is likely to result in the misuse of personal information.

FOLLOW-UP INVESTIGATION/ASSESSMENT IF SECURITY BREACH CONFIRMED

If it is determined after initial investigation that a security breach has occurred, the District shall complete an investigation and assessment of the incident to determine whether the security breach has resulted or is likely to result in the misuse of personal information, which may include the following:

- Depending on the nature of the breach and sensitivity of information, take reasonable near-term steps to mitigate further unauthorized disclosure of personal information and risk of harm.
- Consider designating a lead investigator and investigative team with expertise keyed to the event (e.g. utilization of available District IT professionals if breach involves electronically maintained information, internet, or web resources).
- Interview relevant individuals to learn about the circumstances surrounding the incident and review logs, tapes or other resources.
- Identify individual(s) affected by the breach.
- Determine what personal information has been compromised and how disclosed.
- If applicable, identify affected machines, devices, and IT resources and preserve backups, images and hardware where possible.
- Estimate the likely impact of the compromised data's exposure.
- Utilize professional assistance and consultation as necessary, analyze the likely cause of the breach.
- Coordinate internal and external communications related to the incident. Emphasize maintaining confidentiality during investigative stages of response activities.
- Seek involvement of law enforcement if there is reason to believe criminal activity has occurred.

Notice of Security Breach & Investigation Procedures**NOTIFICATION**

Upon conclusion of the investigation, if it is determined that a security breach has occurred and that misuse of personal information has occurred or is likely to occur, the District shall within forty-eight (48) hours notify the Commissioner of the Kentucky State Police, the Auditor of Public Accounts, the Attorney General, the Commissioner of Education, and the Commissioner of the Department of Libraries and Archives. Within thirty-five (35) days of providing these notices, the District shall notify all individuals impacted by the security breach as provided by law.¹

These notices shall be delayed upon written request of a law enforcement agency that the notices would impede an investigation. Security Breach Forms are located on the Kentucky Finance & Administration Cabinet website:

<http://finance.ky.gov/SERVICES/FORMS/Pages/default.aspx>.

If the investigation determines that misuse of personal information has not occurred or is not likely to occur, the above agency contacts shall be provided notice of the determination. In this case, notice to affected individuals is not required, but the District should maintain records reflecting and supporting the determination.

CONTRACTS WITH NONAFFILIATED THIRD PARTIES - INFORMATION SECURITY

On or after January 1, 2015, agreements calling for the disclosure of “personal information” to nonaffiliated third parties shall require the third party contracting with the District to follow information breach and security standards at least as stringent as those applicable to the District.

Contracts with such third parties shall specify how costs of data breach investigations and notices are to be apportioned.

OTHER PRIVATE INFORMATION

In the case of breach of information made private by law that does not fall within the definition of “personal information”, the District may engage in similar investigative, response, or notification activities as provided above. Alternatively, the District may, after reasonable investigation, provide notice to the individual whose restricted personal information has been acquired by an unauthorized person. Notification will be made in the most expedient time frame possible and without unreasonable delay, except when a law enforcement agency advises the District that notification will impede criminal investigation. Notification should be provided to the individual within three (3) working days of discovery of the breach but no later than thirty (30) working days.

Depending on the number of people to be contacted, notification may be in the form of a face-to-face meeting, phone call, posting on a Web site or sending a written notice to each affected person’s home. Notice should include the specific information involved and, when known, an estimate of how long it has been exposed, to whom the information has been released and how the breach occurred. In addition, the individual should be advised whether the information remains in the physical possession of an unauthorized person, if it has been downloaded or copied, and/or, if known, whether it was used by an unauthorized person for identify theft or fraud purposes.

Notice of Security Breach & Investigation Procedures

REFERENCES:

¹KRS 61.933

KRS 61.931; KRS 61.932

702 KAR 001:170

Data Security and Breach Notification Best Practice Guide

Review/Revised:8/8/2016