Data Breach Procedure - Kentucky Department of Education

In the Event of Data Compromise, Loss, or Exposure

Version: 2.2
Last Updated: 10/07/2015
By: Robert Hackworth
KDE Security Program Manager

Department of Education
Office of Education Technology
300 Sower Blvd.
Frankfort, KY 40601
(502) 564-2020

Revision History

Version	Date	Updated by	Description of Revision
.2	2012/05/07	R. Hackworth	Revise Draft. Include sample notification letter, identification of breach.
1.0	2014/01/06	R. Hackworth	Revise draft. Include data checkboxes. Remove references to districts.
1.5	2014/01/13	R. Hackworth	Revise draft. Create appendices and move form content there.
2.0	2014/12/29	R. Hackworth	Revise draft. Brought into alignment with current version of KDE Affidavit of Non-disclosure; added HBs 5 and 232 into scope.
2.1	2015/03/10	R. Hackworth	Revise draft. Added PTAC FERPA breach notification clarifications.
2.2	2015/05/05	R. Hackworth	Revise draft. Added data breach example to appendices.
2.3	2015/10/07	R. Hackworth	Finalize. Added tips to avoid breach; deleted draft notification letter; deleted forensic investigation procedures – too detailed.

Objective:

To have in place procedures to notify affected individuals of unintentional exposure, loss or compromise of sensitive or confidential information.

Scope:

Paper and electronic data stores under supervision of KDE are to be included in this process as described in KY HB 341 and Kentucky Revised Statute (KRS) 61.932 (2014 House Bill 5).

Exposure of student data entrusted to a 3rd party vendor will be dealt with as described in the terms of the contract with that vendor and Kentucky Revised Statute (KRS) 365.734 (House Bill 232).

Persons Affected:

Data Users - KDE staff, contractors, contracted vendors, network administrators, security administrators and database administrators who use or maintain KDE network and data systems and information contained within.

Affected individuals - Personally Identifiable Information (PII) on individuals, including but not limited to students, educators, school staff, and KDE staff whose sensitive or confidential information was exposed, lost or compromised.

What is a Data Breach?

Per KRS 61.931, a data security breach is defined as

1. The unauthorized acquisition, distribution, disclosure, destruction,

manipulation, or release of unencrypted or unredacted records or data that compromises or the agency or nonaffiliated third party reasonably believes may compromise the security, confidentiality, or

2. The 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 the agency or nonaffiliated third party reasonably believes may compromise the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one (1) or more individuals.
3. "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 subject to unauthorized disclosure.

“Data breaches can take many forms including

- hackers gaining access to data through a malicious attack;
- lost, stolen, or temporarily misplaced documents or equipment (e.g., laptops, mobile phones, portable thumb drives, papers, etc.);
- employee negligence (e.g., leaving a password list in a publicly accessible location, technical staff misconfiguring a security service or device, leaving a printout on the printer, etc.); and
- policy and/or system failure (e.g., a policy that doesn’t require multiple overlapping security measures—if backup security measures are absent, failure of a single protective system can leave data vulnerable).”

-Privacy Technical Assistance Center. *Data Breach Response Checklist*. 2012. www.ed.gov/ptac

What to Do in Case of Suspected Data Breach:

1. Report, immediately within twenty-four (24) hours, any known reasonably believed instances of missing Personally Identifiable Information that has been stolen, inappropriately shared, or taken off-site to:
    a. your immediate supervisor, Associate Commissioner, and
    b. your Office’s Data Controller, found here
    c. the Division of Human Resources if a KDE employee, or
    d. the KDE Office for whom work is performed under the contract if a KDE contractor or an employee of a KDE contractor.

2. Review Appendix A. of this document, noting whatever details you can. This will assist with ongoing investigations.

3. If the suspected breach also involves stolen KDE property, such as a laptop computer, tablet, external hard drive, etc., a police report will be required.

If you are the supervisor or Associate Commissioner of an employee who has reported a potential data breach, you must escalate breach notification within 1 business day. To escalate the issue and trigger breach investigation and reporting, contact any one of the following:

1. Associate Commissioner, Office of KIDS, or
2. Director, Division of Enterprise Data, Office of KIDS, or
3. Security Program Manager, Office of KIDS.

It is the responsibility of one of these staff to make certain that the "Determined Breach Notification Form" is submitted to the Commissioners of the Kentucky State Police, the State Auditor, the Attorney General, and others, within 72 hours of determination or notification.

A this time, FERPA does not add any breach notification requirements, leaving those requirements up to each state:

"As stated in the preamble of the 2008 amendment to the FERPA regulations: "The [U.S.] Department [of Education] does not have the authority under FERPA to require that agencies or institutions issue a direct notice to a parent or student upon an unauthorized disclosure of education records. FERPA only requires that the agency or institution record the disclosure so that a parent or student will become aware of the disclosure during an inspection of the student's education record. … FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR 99.32(a)(1). In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft" (Family Educational Rights and Privacy, Final Rule, 73 Federal Register 74843-74844 [December 9, 2008])."

-Privacy Technical Assistance Center. *Data Breach Response Checklist*. 2012. www.ed.gov/ptac

What is Personally Identifiable Information?

KRS 61.932 defines "personal information" as:

- 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 required security code, access code, or password, permits access to an account;
- A Social Security number;
- A taxpayer identification number incorporating 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.

FERPA, or The Family Educational Rights & Privacy Act, has a slightly different definition of PII, as it is focused solely on students.

- The student's name, and name of the student's parent or other family members;
- 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
    - student's date of birth,
    - place of birth, and
    - mother's maiden name.
- 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.
- Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

What Can I Do to Not Become a Victim of a Data Breach?

1. Leave PII at work. Keeping PII on your laptop, tablet, USB drive, etc. is tempting fate. It can't be stolen or accidentally shared if it isn't there in the first place.
2. Keep your phone, laptop, tablet, USB drives, and the purses, satchels, and backpacks that might contain them, out of sight while in your car, even with the doors locked. Locks only keep the honest people out, and a determined thief will break your window to steal your devices.
3. Be very suspicious of any pop-up windows on your computer or emails warning of viruses or urging you to call a helpdesk. Always contact the KETS Service Desk at 502-564-2020 or 866-538-7435 to verify these claims.
4. Double-check all your files before sharing them, especially if you are not the author. PII can hide in spreadsheets, on lists or forms in a document, or even screen shots in a presentation.
5. Contact someone in the Office of KIDS, Division of Enterprise Data if you need to share information that might be PII, or if you receive PII that you weren't expecting from another source.
6. Use strong passwords that can't be easily guessed, especially for systems that contain PII.
7. Learn how to encrypt files. If files with PII are encrypted, there's almost no chance they can be read except by the people with a password to the encrypted file. Encryption is easy and can even be free! Contact the KETS Service Desk for more information and options.

- **Appendix A: Detailed Description of Breach**

Date & Time Suspected Breach was Discovered:

Data Elements Involved:

☐ First Name or First initial	☐ Last Name
☐ Birth Date	☐ Driver's License Number
☐ Employee Number	☐ Unique Student ID
☐ Password	☐ Account Name or Number
☐ Social Security Number	☐ Credit/Debit Card Number
☐ Tax Identification Number	☐ Medical Information
☐ Email Address	☐ Network/System Information
☐ Physical Address	☐ Other/Unknown:

Data Systems Involved:

☐ KSIS	☐ District Financial
☐ Human Resources	☐ KDE Financial
☐ Student Assessment	☐ Individual Learning Plan (ILP)
☐ SRIM	☐ Nutrition
☐ Legal	☐ E-Rate
☐ Workstation	☐ Other/Unknown:

Type of Breach:

Physical	**Electronic**
☐ Hardcopy/Paper	☐ Phishing/Email
☐ Laptop	☐ Stolen Login Credentials
☐ Phone	☐ Data Theft
☐ Tablet/Slate	☐ Unauthorized Data Change
☐ Desktop/Server	☐ Unauthorized Data Destruction
☐ Other/Unknown:	☐ Other/Unknown:

Appendix B: Hypothetical Security Breach Scenarios

The “Looted Laptop”

1. You have decided to go out to dinner before getting home, and leave your laptop in the trunk, where it’s safe.
2. Unfortunately, you leave your car unlocked or it’s broken into while you are eating, and the thieves relieve you of $3 in change from the ashtray, a leather jacket from the backseat, and they open your trunk and take your KDE-assigned laptop. However, they don’t take your copy of “Rio” by Duran Duran. SCORE! ☺
3. You come out from dinner, realize your car has been broken into, and call the police and file a report.
4. You quickly assess whether there was anything important on the laptop, and decide it did NOT have student or staff PII, but it DID have timesheet information – YOUR information. Then you remember that there is a KDE Data Breach Notification Procedure form, and you decide to review it tomorrow when you get to work.
5. The next morning, you read the data breach procedure and call or meet face to face with (because email is too slow and doesn’t ensure a response) your direct supervisor/manager and describe what happens. This person makes certain that the office’s Associate Commissioner is made aware via a phone call or face to face conversation.
6. The Associate Commissioner then calls, or designates someone to call, the KDE Chief Information Officer (David Couch), the Division of Enterprise Data Director (Dede Conner) or the Chief Security Officer (Bob Hackworth) to relay that there has been a potential or probable breach. Again, this must be a call or face to face.
7. David, Dede, or Bob assess the situation and decide what needs to happen next.
8. Bob contacts theft victim and goes through a more detailed procedure to answer any questions and ensure we have the information we need in order to move forward. Odds are, the laptop will never be recovered, but the good news is there was a backup of your data, and a careful examination determines that there was no PII, other than your timesheet data, which means it’s POSSIBLE that you should start keeping an eye on your credit report.
9. If a data breach is suspected, multiple notifications, as defined in the body of the Process Document, will be sent to various commissioners of state agencies including, but not limited to the Department of Education, the Attorney General, the Auditor of Public Accounts, and the Commonwealth Office of Technology.

The “Email of Doom”

1. It’s late in the day; you’re still at work and the sun is shining. Just as you get up from your desk and leave, you hear the familiar “ding” of an email message. “OK. Just one more,” you think. It’s from your buddy down the hall, who wants you to send a spreadsheet with aggregate student counts to your district distribution list. It won’t take long.
2. You click “Forward,” add a short message to the email body, put the distribution list in the “To:” field and hit “Send.” Done. Time for a short walk in the SUNSHINE then on to the house and dinner!
3. The next morning, the sun is shining and that donut/vada/youtiao with coffee tasted WAY better than it should’ve as you walk to your desk. The red light on your phone indicating that there’s a message barely registers.
4. As your email opens, you notice LOTS of new messages this morning. Many of them have ALL CAPS in the subject line saying things like “STUDENT PII SENT” and “DATA BREACH!!!” and they seem to be related to that email you sent for your buddy yesterday. Uh oh.
5. Your breakfast starts to churn uncomfortably in your stomach as you look in the “Sent” folder for THAT email and then open it up.
6. The attachment. You open it. As expected, the spreadsheet has the aggregate student counts on it, so SURELY there must be some mistake? Then you see it. THEM. TABS. Your hand trembling, you click on a tab and there they are: names; SSNs; birthdates; etc. The tabs have detailed student data from half the high schools in the state! The aggregate data were being pulled from these tabs.
7. Because you are already familiar with KDE’s data breach procedure, you immediately contact your Division Director via phone, who then attempts to contact your Office’s Associate Commissioner. In the meantime, you use the checklists in Appendix A to begin assessing the situation.
8. Your Associate Commissioner is out, so your Division Director contacts David Couch/Dede Conner/Bob Hackworth via telephone or face to face, and describes the issue as best as possible. You are able to provide the Appendix A with the helpful information.
9. David, Dede, or Bob assess the situation and decide what needs to happen next. This one is pretty bad. KDE will need to send out notifications to the parents of all the students involved in the data breach and that’s just the beginning. This will most likely be a long and painful process not just for the agency, but more importantly for all of the parents of the students, who may feel as though the security of their children’s identities has been irreversibly weakened or even lost. This will impact everyone for months if not longer.
10. A few days later, as your job finally begins to get back to normal, you wish you could turn back time. You wish you had taken the extra minute to really look at that attachment before you forwarded it out.