Data Security and Personal Information Privacy

- *Adapted from KDE Data Governance materials with permission from Robert Hackworth, Chief Security Office (http://education.ky.gov/districts/tech/Pages/Data-Security-Privacy.aspx)*

On January 1, 2015, a new state law, the Personal Information Security and Breach Investigation Procedures and Practices Act (KRS 61.931, et seq.) went into effect. This legislation is more commonly known as "House Bill 5." This Act concerns the protection of personal information and applies to every state agency, including KDE, every public school district, and every vendor with which we have contracts.

What do we control that are considered Personal Identifiable Information (PII)?

- Social Security Numbers
- Health records
- Free and Reduced status
- Student/Employee records

Data Risks –

Unlike the private sector or most other parts of government, a very high percentage of the data elements collected and used in P-12 schools are not considered confidential and are usually made directly accessible to any public citizen either instantly through a variety of electronic means (e.g., Web sites at schools, district offices, the Kentucky Department of Ed and the U.S. Education Department) or very quickly in response to open records requests that must be provided in paper or e-mail form.

The majority of the truly private P-12 data is controlled by district staff, who control the permissions to these areas, systems and services. Most reside:

· physically (on paper within cabinets, on electronic files or workstations) within the district
· virtually with cloud services as they increase in popularity

Most of the time, if there is an exposure of this type of restricted personal data, such as a student's medical records or a teacher's SSN, it happens accidentally (e.g., confidential personal data is printed to an unintended printer in a building, e-mailed to the wrong person or group or placed on an incorrect Web site). Also, the number of people who accidentally see confidential data that they should not be viewing tends to be limited to a small group; most of which disregard or destroy what they have seen because they do not realize that it is restricted personal data.

There are times where there are intentional attempts (e.g., a laptop or cabinet drawer containing paper files is stolen from a school, someone is just curious about a fellow employee's personal information) to access restricted personal information by unauthorized people who do not have a true need to know.

The cornerstone of improving data security is basic awareness among all staff. To address awareness and system-wide planning and action, the Barren County Schools will focus on a three leveled approach:

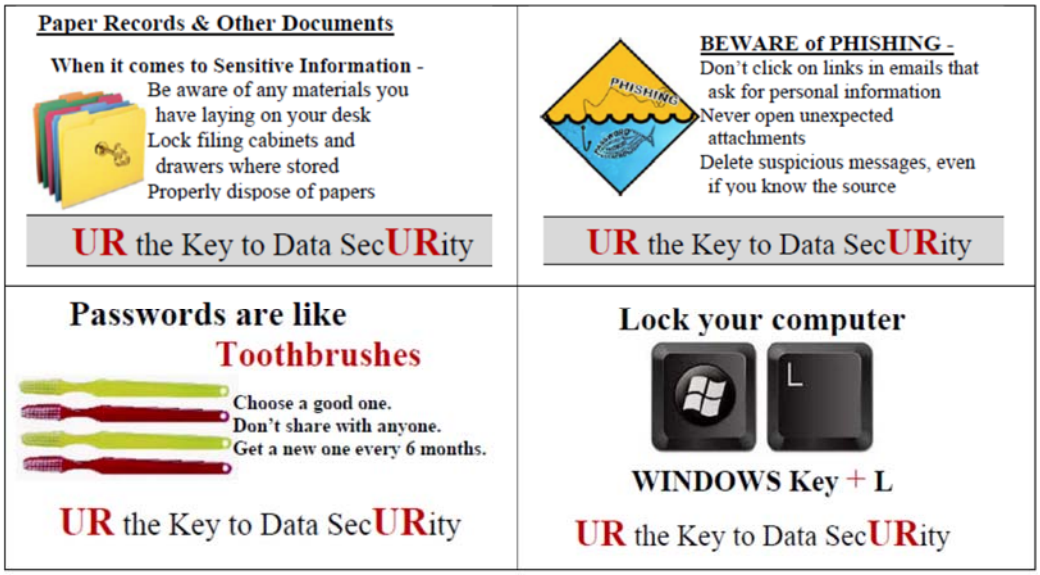
Staff Awareness – general all staff and specific for data secure staff (directors, sec, counselors, principals, key district staff); followed by tips & reminders during the year (Tip Card – Windows + L; password protect a file; redact Pii from document; secure print)

Classify Data & Data Levels – identify data stewards; location/type of PII by department; review retentions schedule; securely destroy PII; data diets;

Security Systems – time outs set on access to critical programs; lock screens set to less than 15 min; access rights reviewed (limit access to SSN); secure locations & locking cabinets for PII and working location for files in use.

There are actions that all staff can take now to improve data security in our schools and district:

- **Create computer and system passwords that are "strong"** (not dictionary words), changed often not shared (or written down).
- Infinite Campus and other databases must be **password protected and not left open** when not in use.
- **Setting "lock" screen timers**, auto-log off timers, etc. to the shortest amount of time as possible – 10 to 15 minutes suggested. Use the windows lock screen shortcut (**windows key + L**) to lock computer when you leave work station.
- **All contracts with vendors must comply** with new requirements of state and federal laws, including KRS 61.931 (or House Bill 5). This includes APPS, programs, and on-line services.
- Securely storing all paper documents with student information **in locked cabinets and out of sight** of those without "need to know." **Securely destroy docum**ents when they are no longer used.
- **Do not email or transmit personally identifiable information to others.**



Additional training and resources will be shared with staff with higher levels of data access. Additional awareness and security measures will be developed and implemented.

When PII that is improperly obtained, and it is determined to likely result in the harm of one or more individuals, the breach of data security must be reported according to specific steps that are outlined by KDE and the state statutes that have been enacted.

Cloud Provider Agreements

The new KRS 365.734 indicates that Cloud Providers (online services, mobile apps, etc) must comply with the terms of the new laws. They must protect "Student data" and defines that as "any information or material, in any medium or format that concerns a student and is created or provided by the student in the course of the student's use of cloud computing services, or by an agent or employee of the educational institution in connection with the cloud computing services." The KRS goes on to say that "Student data includes the student's name, e-mail address, e-mail messages, postal address, phone number, and any documents, photos, or unique identifiers relating to the student."

Impact on Classroom Teachers

All staff must be aware that all 3rd party vendors must agree to the terms of this law in order to provide services to K-12 districts. Be cautious of services that you want to utilize that may be collecting PII for students. Agreements must specify the compliance with KRS 365.734 (HB 5).

A Kentucky Educator's Guide to TOP SECRET Personal Information and Data Breach Awareness

Advancing technology like email, cloud systems, and social media have made it easier than ever to use or lose vast amounts of data very quickly. Many folks aren't aware of the risk/threat of a data breach, or worse, don't know what information is TOP SECRET. Breaches are NOT inevitable. They DO pose a significant risk to students, districts, and ourselves. This handout is a quick introduction on WHAT to protect, and HOW best to do so.

WHAT IS PERSONAL INFORMATION (P.I.)? HINT: IT'S TOP SECRET!

No matter what it's called, it might be easier to just think of it as "**top secret.**" Top secret data is the stuff we need to keep secured and private because it could do the most harm to the person it's about if it was stolen or accidentally exposed. Let's focus on the 3 following privacy laws: KRS 61.931 (2014's House Bill 5), KRS 365.734 (2014's House Bill 232) and the Family Education and Rights Privacy Act (FERPA).

EVERYONE

STUDENTS ONLY

KRS 61.931 – 934 (House Bill 5)	KRS 365.734 Section 2 (House Bill 232)	FERPA	What is a Data Breach?
1st name or initial AND last name or biometric record PLUS 1 or more of the following: An account, credit or debit card # with an access code, PIN, or password A Social Security Number Taxpayer ID that incorporates SSN Driver's license or any state-issued ID Passport number or an federally-issued ID Individually identifiable health information	Any information or material, in any medium or format, that concerns a student and is created or provided by the student in the course of the student's use of cloud computing services, or by an agent or employee of the educational institution in connection with the cloud computing services. Student data includes: Student name Email address Postal address Phone number Any documents, photos, or unique identifiers relating to the student	Student name Name of the student's parent or other family members Postal address of student or student's family Personal ID, such as SSN, student number or biometric record Indirect IDs, i.e. DOB, place of birth, 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	A data breach is the unauthorized (whether stolen or lost) release of top secret data that can be reasonably believed to put the security, confidentiality, or integrity of the data a risk and cause harm to 1 or more individuals. Once a person's data are lost or stolen, they can be sold multiple times to others who then steal the victim's identity, open fraudulent bank accounts or credit cards, or obtain healthcare. It can leave the victims, which includes children, many thousands of dollars in debt, depending on how long it goes on undetected.
If these data are exposed, missing or stolen, IT IS a breach	**Data not to be shared with vendors without appropriate use agreement**	**If these data are exposed, missing or stolen, IT MAY BE a breach**	

IS A STUDENT ID (STATE STUDENT IDENTIFIER - SSID) TOP SECRET?

The Family Policy Compliance Office, which administers FERPA, says that student identification numbers aren't top secret as long as they "cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the student's identity, such as a personal identification number (PIN), password, or other factor known or possessed only by the student or authorized user."

KDE encourages use of the student ID (SSID) without other identifiers when possible. Do not send SSNs, full names or more information than is absolutely necessary when requesting assistance from KDE.

Click here for more information about data privacy and security.

THE MOST COMMON DATA BREACHES, AND HOW TO PREVENT THEM

Human error is the most common enabler of a data breach. While hackers get most of the spotlight, they wouldn't be so successful (by a WIIIIIDE margin) if, frankly, all of us weren't making it so easy for them. Here are the four most common types of data breaches in Kentucky's K12 environment, and how to prevent them.

LOSS OR THEFT OF A USB THUMBDRIVE, LAPTOP, TABLET, OR SMARTPHONE CONTAINING P.I.

How to prevent the breach:

- DO NOT save or store top secret information on these devices in the first place
- DO NOT leave valuables on the seat or visible in your car; lock them in the trunk
- Encrypt the device, or the top secret Information on your device. If it's encrypted, it does not cause a data breach as long as the password isn't available

Example: P.I. is downloaded to a laptop and then the laptop is lost or stolen from your car or at a school function, it won't matter that the thief was only looking to sell the laptop; if there's P.I. on the device, that's a breach.

PHISHING ATTACKS

How to prevent the breach:

- DO NOT share your password with anyone. No reputable company will EVER ask for your password
- DO NOT click on links or documents you aren't expecting - Be savvy
- DO NOT casually browse the web or check personal email from a computer or server that is used for collecting and managing top secret data, such Infinite Campus, financial, or cafeteria programs

Phishing is a crime in which the attacker tries to trick you into downloading malware or sharing private information, such as password or SSN, by masquerading as a helpdesk, a company or even a person you know. If you fall for their trick, then the attacker has access to your accounts, your computer, or both.

POOR OR SHARED/STOLEN PASSWORDS

How to prevent the breach:

- DO NOT use passwords based on "password" or the names of the seasons, months, family members, pets, or sports teams. Everyone uses them so they are VERY predictable and the first ones a hacker will try
- Use long AND memorable passwords or passPHRASES like "4sCORE&5evnYrs" (four score and seven years) which is easy to remember, but cannot be easily guessed

HINT: No one enjoys using passwords. Most people create poor, easy to remember passwords or keep them taped to monitors or "hidden" under the keyboard. Out of the possible billions of passwords, 90% of people use the same 50 passwords or styles of passwords. This makes the password memorable, but also very easy to predict.

ACCIDENTAL SHARING OF P.I.

How to prevent this breach:

- DO NOT send or forward emails or documents without first checking for P.I. Once sent, that email and everything in it is YOUR responsibility, even if you are just forwarding it along.

Examples: Student reports, timesheets, job applications, screenshots for trainings or hidden columns and tabs in a spreadsheet are very common ways P.I. are accidentally shared.