TOP SECRET

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!

From a legal perspective, KRS 61.931 (House Bill 5) states "Personal Information" means 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:

This!

- 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;
- A Social Security number;
- A taxpayer identification number that incorporates a Social Security number;
- A driver's license number, state identification card, 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 (FERPA), as amended 20 U.S.C. sec. 1232g.

Is A Student ID (State Student Identifier - SSID) top secret?

The Family Policy Compliance Office, which is responsible for administering FERPA, states that a student identification number can be considered directory information (not P.I.), "but only if the electronic identifier 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."

If using the SSID to request assistance from KDE or a vendor, KDE encourages use of the student ID (SSID) without other identifiers. Do not send SSNs, full names or more information than is absolutely necessary.

Click here for more information about data privacy and security.

What is a Data Breach?

According to KRS 61.931, a data breach is the unauthorized (whether stolen or lost) release of P.I.

that can be reasonably believed to jeopardize the security, confidentiality, or integrity of the data and cause harm to 1 or more individuals. A data breach harms the victims because their information is lost and a crook can sell the information multiple times to other crooks who then steal the victim's money, identity, open fraudulent bank accounts or credit cards, or even obtain healthcare. It can leave the victims, which can include children, thousands or even hundreds of thousands of dollars in debt, depending on how long it goes on undetected.

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 WIIIIDE 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 personal 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 Personal Information on your device. Encrypted P.I., if lost or stolen, 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 P.I., such as one running 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. It can happen via email, webpage or phone. 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.