A Quick 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? HINT: IT'S TOP SECRET!

No matter what it's called, it might be easier to just think of personal information 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 or organization it's about if it was stolen or accidentally exposed.

Let's focus on the 3 following privacy laws: KRS 61.931 or House Bill 5, KRS 365.734 or House Bill 232, and the Family Education and Rights Privacy Act or FERPA.

KRS 61.931 OR HOUSE BILL 5 FROM 2014 (impacts everyone)

This Kentucky law that went into effect on January 1st 2015 applies to anyone whose data are being stored by state or city government, public universities or public schools. If any of the following data are exposed, it would be considered a data breach. It defines **TOP SECRET** data as the first name or initial and the last name or biometric record such as a fingerprint plus one or more of the following:

- An account, credit or debit card number with an access code, Personal Identification Number or PIN, or password
- A Social Security Number
- A taxpayer ID that incorporates the Social Security Number
- A driver's license or any state-issued identification
- A passport number or a federally-issued identification
- Or individually identifiable health information

KRS 365.734 OR HOUSE BILL 232 FROM 2014 (impacts students only)

This Kentucky law that also went into effect on January 1st 2015 applies to vendors who provide cloud services and store student data. These data are not to be shared with or by vendors without the proper consent forms. It defines STUDENT data 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. Student data includes:

- Student name
- Student email address
- Student postal address
- Student phone number
- Any documents, photos, or unique identifiers relating to the student

FAMILY EDUCATION AND RIGHTS PRIVACY ACT OR FERPA (impacts students only)

FERPA does not specify data that will cause a data breach. However, exposure of certain information could be a FERPA violation for the school, and the school may want to call that a data breach. FERPA defines student data as:

- Student name
- Name of the student's parent or other family members
- Postal address of the student or student's family
- Personal ID, such as Social Security Number or biometric record
- Indirect identifiers such as Date of Birth, 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.

If any of those data are defined by the school as Directory Data, then they would not contribute to a FERPA violation or data breach.

IS A STUDENT ID (STATE STUDENT IDENTIFIER - SSID) TOP SECRET? The Family Policy Compliance Office, which administers FERPA, says that student identification numbers, which are known as a student's SSID in Kentucky, 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 without other identifiers when possible. Do not send Social Security Numbers, full names or more information than is absolutely necessary when requesting assistance from KDE.
Click on this sentence for more information from the Kentucky Department of Education about data privacy and security.

What is a Data Breach?

A data breach is the unauthorized, such as 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 one 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.

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 wide 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 PERSONAL INFORMATION

How to prevent this 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, itdoes 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 foryour password
- DO NOT click on links or documents you aren't expecting - Be savvy
- DO NOT casually browse the web or check personal emailfrom 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 scoreand 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.
- Before taking a screen shot to send to someone else, make sure no P.I. is visible on thescreen.

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.