Bullitt County Public Schools
Moving Forward

It's a NEW YEAR, Think before you Share

Exercise caution with student and personal information.

What is sensitive data, or Personally Identifiable Information (PII)? *In 2014, 93 percent of data breaches were due to human error, poor processes and systems in place, and lack of care when handling data.*

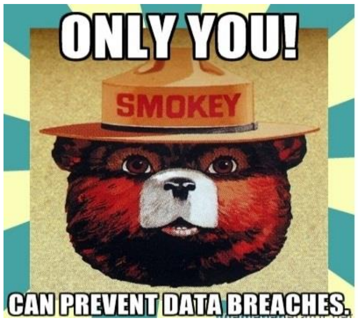
First Name or First Initial and Last Name in combination with:

- Social Security Number
- Driver License Number, State ID, or other individual identification number issued by any agency
- Passport Number
- Identifiable Health Information

Examples:

John Doe 405-00-0000 = PII
J Doe 405-00-0000 PII
J Doe Blue Cross ID# 123-456789 PII
John Doe

- Use strong passwords by combining uppercase, lowercase, numbers and special characters with at least *8 characters* in length.
- Change your passwords frequently
- Lock your desktop or laptop computer every time you step away
- Do not give your password to students, subs, or anyone
- Teachers - log off computers before allowing students to use them
- Don't put your username or password of any programs on your monitor or near your computer in classrooms
- Avoid using flash or thumb drives. (If you must use them, use Windows Bitlocker to encrypt the data.)
- Substitute Google Drive for a flash/thumb drive. (It's free, available anywhere in the world, and your BCPS account provides you unlimited storage.)
- Exercise caution when submitting data to websites (Does it meet the test for PII?).
- If you have a district laptop, do not store any PII on the local hard drive.
- If you are on public WiFi, *do not access data that has sensitive or PII data*. Wait until you are on a secure network (BCPS or at home).
- Avoid saving data in too many locations (Dropbox, Google Drive, One Drive, Flash/Thumb Drives, etc.)



In addition, avoid the following risky situations:

- Emailing a list of student names and ID's to another teacher
- Emailing a medical release form to all teachers for a child that has just been released to return to school (Remember, emails can be forwarded to ANYONE!)
- Pulling an ad hoc report from Infinite Campus that has student names and ID's or socials and saving to your desktop, or emailing to staff.
- Leaving a flash/thumb drive on the desk in your classroom, or in the USB port of the computer
- Putting PII, district or student data on flash/thumb drives, then it gets lost or stolen (because they were unencrypted and in a purse)
- Leaving student medical or other confidential information on your desk or in an unlocked drawer
- Sharing a file with PII with the wrong person
- Having laptops with PII taken from parked cars (store them out of sight or in trunk)
- Responding to phishing "urgent" requests via email or while browsing the web, "requiring" action…?