Bullitt County Public Schools
Instructional Technology
1040 Highway 44 East
Shepherdsville, Kentucky 40165
502-869-TECH

Moving Forward

MEMO

To: Jesse Bacon, Superintendent

From: Jim Jackson, District Technology Coordinator

Date: Thursday, July 05, 2018

Re: School and district data security and breach procedures

According to new regulations 702 KAR 1:170 Section 3, school districts are now required to publicly acknowledge a review of the Data Security and Breach Notification Best Practices Guide.

This past year, we submitted a test "Phishing" email and about a third of the district users submitted personal information in response to that email. In addition, we had a security audit of our network and technology environment and I will share those results with the Board in August. We are making good progress at network and data security; however, we still have room to improve.

The biggest threat comes from weak passwords and users falling victim to Phishing frauds. As a result, I have asked for the mandatory addition of "Password Security Basics", and "Email and Messaging Safety", with optional training for "Browser Security Basics" with the mandated district trainings.

We will also implement self-service password resets for users that forget their passwords. Along with this, we will implement forced password changes two times a year, with an ultimate goal of once every quarter and possibly more frequently. The threats of security breaches and cybercrime are becoming too frequent, and we need to address best practices to protect our district students, staff and administration.

We have posted pertinent information on the technology webpage, which includes a "Security" tab, which covers procedures and protocol for a data breach. We remind district staff at the begging of school and after Christmas break on what actually constitutes PII, and remind them to exercise caution when sharing data. This email includes a simplified one-page document for quick reference, which will help define what data are considered "sensitive" or Personally Identifiable Information (PII).

We will continue to remind district employees of the importance of protecting student data, and to remain vigilant at identifying scams and protecting all district data and passwords.

It's a NEW YEAR, Think before you Share

Exercise caution with student and personal information.

- 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.)

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

- 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...?