



FLOYD COUNTY BOARD OF EDUCATION  
Anna Whitaker Shepherd, Interim Superintendent  
442 KY RT 550  
Eastern, KY 41622  
Telephone (606) 886-2354 Fax (606) 886-4550  
www.floyd.kyschools.us

Linda C. Gearheart, Board Chair - District 1  
William Newsome, Jr., Vice-Chair - District 3  
Dr. Chandra Varia, Member - District 2  
Keith Smallwood, Member - District 4  
Steve Stone, Member - District 5

Date: July 16, 2021


**Consent Agenda Item (Action Item):** Approve the Floyd County Data Security Best Practices Presentation

**Applicable State or Regulations:** BOE Policy 01.11 General Powers and Duties of the Board

**Budget/Financial Issues:** N/A

**Recommended Action:** Approve as presented

**Contact Person(s):** S. Denise Isaac, Chief Information Officer

  
Director

  
Superintendent

**Date:**

# **Data Security & AUP**

**ALL Employees**

## Points of Emphasis

- ❑ Change password regularly ; District Password Policy & implementation of 15-character & multi factor authentication policy. DO NOT USE passwords based on “password” or the names of the seasons, months, family members, pets, or sports teams.
- ❑ DO NOT SEND emails or documents without first checking for Personal Information. ONCE SENT, THAT EMAIL IS YOUR RESPONSIBILITY (*even if you just forward it*)
- ❑ NEVER share your password (*Students should NEVER have your password*)
- ❑ DO NOT OPEN EMAILS or LINKS from email accounts that you don't know or don't look like reputable agencies. *Call IT to confirm.*
- ❑ NEVER SHARE PERSONAL INFORMATION ONLINE
- ❑ Use Student SSID without other identifiers
- ❑ IF BOE Email is on personal devices, we ask that you have a passcode on any device (ex: personal phone) to protect any PI or other confidential info visible through district email. Protect ALL PI info, student, employee, family, etc.

## What is P.I.?

- ❑ **Personal Information: 1st Name or initial AND last name PLUS:  
Account or credit card #, PIN or password, Social Security Number, Taxpayer ID, Driver's License, Passport Number, Identifiable Health Information**



# Data Security Resources

## [KDE Data Security and Breach Notification Best Practice Guide](#)

## [KY Educator's Guide: Personal Information & Data Breach Awareness](#)

**TOP SECRET**

### 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 WIIIDE 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 as 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.

## Data Security

- Data Security Best Practices
- Signature of completion: Google Form for ALL Staff (Certified & Classified)
- [Review AUP](#)

## Devices

## Phishing