To: *Fort Thomas Independent Schools Board of Education*
Brian Robinson, FTIS Superintendent

From: *Kevin Hester, FTIS Network Administrator*
Jody Johnson, FTIS Director of Technology and Information

Date: *August 8, 2024*

Re: *Data Security and Breach Procedures*
Annual Public School District Acknowledgements of Best Practices
KAR 702 001 170

The purpose of this annual review is to provide assurances that Fort Thomas Independent Schools has reviewed the best practices and guidelines issued by the Kentucky Department of Education regarding data protection and procedures to institute in the case of a data breach.

The following points outline some of the practices put into practice, as well as additional actions that go beyond the scope of the KDE Guidelines.

INHERITED SAFEGUARDS

- Data Privacy, Security, and Breach Best Practices and Guidelines published by KDE (implemented and reviewed annually) and input from KDE Security Team
- Centralized directory service for account management
- IP Address management
- Centralized firewall

CONTINUING PRACTICES AT DISTRICT LEVEL

- Assurances that all subscriptions and services comply with FERPA, CIPA, and COPPA
- Secure password policies and Multi-Factor Authentication for all employees
- Student Information System user groups and rights assigned as needed
- Annual Safe School Training for data security for all teachers
- Device and MDM selections
- Single Sign On subscriptions when available
- Physical security of networking components
- Immutable off-site server backups

DISTRICT UPGRADES

- Annual reminders and education on phishing attacks
- Improving Disaster Recovery Plan
- Increasing security by upgrading existing network
- Enrollment in Student Data Privacy Consortium (SDPC)
- Enrollment in Cyber Hygiene Vulnerability Scanning by Cybersecurity and Infrastructure Security Agency (CISA)