To:
Fort Thomas Independent Schools Board of Education
Brian Robinson, FTIS Superintendent
From:
Jody Johnson, FTIS Director of Technology and Information
Kevin Hester, FTIS Network Administrator
Date:
August 4, 2022
Re:
Data Security and Breach Procedures
Annual Public School District Acknowledgements of Best Practices
KAR 702 001 170

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

The following outlines some of the points 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)
- Centralized directory service
- IP Address Management
- Centralized firewall

CONTINUING PRACTICES AT DISTRICT LEVEL

- Assurances that all subscriptions and services comply with FERPA, CIPA, and COPPA.
- Enhanced password policy for district employees.
- Student Information System user groups and rights assigned as needed.
- Annual Safe Schools Training for data security for all teachers.
- Device and MDM selection.
- Process of removing outgoing user accounts.
- Rostering portal and Single Sign-On.
- Physical Security of Networking Components

DISTRICT IMPROVEMENTS

- Additional emphasis and education on handling phishing attempts
- Move to Multi-Factor Authentication for employees
- Review and revision of Acceptable Use Policy
- Improved Cybersecurity implementations
- Back up systems
- Network updates