



# *Data Governance Policy*

# Dothan City Schools Data Governance Policy

## I. POLICY

- A. It is the policy of Dothan City Schools that data or information in all its forms--written, electronic, or printed--is protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment, software, and practices used to process, store, and transmit data or information.
- B. The data governance policies and procedures are documented and reviewed annually by the data governance committee.
- C. Dothan City Schools conducts annual training on their data governance policy and documents that training.
- D. The terms data and information are used separately, together, and interchangeably throughout the policy. The intent is the same.
- E. The superintendent and/or his/her designee is authorized to establish, implement, and maintain data and information security measures and procedures. The policy, standards, processes, and procedures apply to all students and employees of the district, contractual third parties and agents of the district, and volunteers who have access to district data systems or data.
- F. This policy applies to all forms of Dothan City Schools' data and information, including but not limited to:
  - A. Speech, spoken face to face, or communicated by phone or any current and future technologies,
  - B. Hard copy data printed or written,
  - C. Communications sent by post/courier, fax, electronic mail, text, chat and or any form of social media, etc.,
  - D. Data stored and/or processed by servers, PC's, laptops, tablets, mobile devices, etc., and
  - E. Data stored on any type of internal, external, or removable media or cloud based services.
- F. The district will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems. Dothan City Schools complies with all applicable regulatory acts including but not limited to the following:
  - A. Children's Internet Protection Act (CIPA)
  - B. Children's Online Privacy Protection Act (COPPA)
  - C. Family Educational Rights and Privacy Act (FERPA)
  - D. Health Insurance Portability and Accountability Act (HIPAA)

- E. Payment Card Industry Data Security Standard (PCI DSS)
- F. Protection of Pupil Rights Amendment (PPRA)
- G. Failure to comply with this policy by students may constitute grounds for corrective action in accordance with Dothan City Schools' policies. Further, penalties associated with state and federal laws may apply. Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:
  - 1. Unauthorized disclosure of PII (Personally Identifiable Information) or Confidential Information.
  - 2. Unauthorized disclosure of a login code (User ID and password).
  - 3. An attempt to obtain a login code or password that belongs to another person.
  - 4. An attempt to use another person's login code or password.
  - 5. Unauthorized use of an authorized password to invade student or employee privacy by examining records or information for which there has been no request for review.
  - 6. Installation or use of unlicensed software on Dothan City School technological systems.
  - 7. The intentional unauthorized altering, destruction, or disposal of Dothan City Schools' information, data and/or systems. This includes the unauthorized removal from DCS of technological systems such as but not limited to laptops, internal or external storage, computers, servers, backups or other media, copiers, etc. that contain PII or confidential information.
  - 8. An attempt to gain access to login codes for purposes other than for support by authorized technology staff, including the completion of fraudulent documentation to gain access.