Washington County Schools

Data Governance Policy

1. Introduction

A. It is the policy of Washington County School Board of Education (WCBE) that information, as defined in all its forms, written, recorded electronically or printed shall be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection shall include an appropriate level of security over the equipment and software used to process, store, and transmit that information.

B. This data governance policy and its procedures shall be documented and reviewed annually by the data governance committee.

C. The WCBE will conduct annual training on the data governance policy and document that training.

2. Scope

The policy, standards, processes and procedures apply to all students and employees of the district, all third parties and agents of the district who have access to district information systems or information.

The policy applies to all forms of information, including but not limited to:

- Speech, spoken face to face, or communicated by phone or radio,
- Hard copy data printed or written on paper,
- Communications sent by post/courier, fax, electronic mail, text, chat and/or any form of social media, etc.,
- Stored and processed by servers, PC's laptops, tablets, mobile devices, etc.,
- Stored on any type of removable media or cloud based services

Data Governance Committee

Ashley Becton	Teacher
Betty Brackin	Administrator
Jeff Ford	District Technology Coordinator
Kay Savage	Counselor
John Dickey	Superintendent
Jamelle Sauls	Principal
Curt Stagner	Principal

Regulatory Compliance

The WCBE will abide by any law, statutory, regulatory, or contractual obligations affecting its information systems.

- *CIPA*, the Children's Internet Protection Act. The WCBE has adopted an Internet safety policy that includes monitoring the online activities of minors; and, the WCBE requires all students participating in on-line activities participate in an Internet safety course about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.
- *COPPA*, the Children's Online Privacy Protection Act. The WCBE requires parental permission for all commercial websites or online services that gather information on students under 13 years old.
- *FERPA*, the Family Educational Rights and Privacy Act. The WCBE protects student information and accords the specific rights as determined by *FERPA* with respect to student data.

Access Control and Compliance

- Data users are expected to respect the confidentiality and privacy of individuals whose records they access; to observe any restrictions that apply to data; and to abide by applicable laws, policies, procedures and guidelines with respect to access, use, or disclosure of information. The unauthorized use, storage, disclosure, or distribution of System Data in any medium is strictly forbidden; as is the access or use of any System Data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy one's own personal curiosity or that of others.
- Each employee of the district will be responsible for being familiar with the district's data security policy as it relates to his or her position and job duties. It is the express responsibility of authorized users and their supervisors to safeguard the data they are entrusted with, ensuring compliance with all aspects of this policy and related procedures.
- Violations of these Data Security Measures may result in loss of data access privileges, administrative actions, and/or personal civil and/or criminal liability.

Data Classification and Access Controls

Student Data	**Authorized Users**	**Web Access**
Student Name	All, as needed	First Name, Last Name Only, except in press release, school newspaper, or C2C
District Student Number	Superintendent, Principal, Counselor, Asst. Principal, Teachers, Student, Parent, CNP, Media Specialist, Technology Coordinator, Federal Programs Coordinator. Also export to approved service providers in order to establish unique identities or accounts – requires Data Governance Committee approval.	No
State Student Number	Superintendent, Principal, Asst. Principal, Counselor, Student, Parent, testing personnel, Technology Coordinator, Child Nutrition personnel, Federal Programs Coordinator	No
Social Security Number	Superintendent, Principal, Counselor, Asst. Principal, Testing Coordinator, Special Ed. Coordinator, Technology Coordinator, Federal Programs Coordinator, CNP Coordinator and appropriate staff, Career Technical Personnel	No
Home Phone Number	Superintendent, Principal, Counselor, Asst. Principal, Student, Parent, Testing Coordinator, Special Ed. Coordinator, Technology Coordinator, Federal Programs Coordinator, Bus drivers, Assigned Teachers, After School Care personnel, Transportation supervisor and Rapid Response system directory	No
Home Address	Superintendent, Principal, Counselor, Asst. Principal, Student, Parent, Testing Coordinator, Special Ed. Coordinator, Technology Coordinator, Assigned Teachers, Federal Programs Coordinator, After School personnel, bus drivers, Transportation supervisor and Rapid Response notification system	No
Ethnicity	Superintendent, Principal, Counselor, Asst. Principal, Student, Parent, Testing Coordinator, Special Ed. Coordinator, Technology Coordinator,	No

	Assigned Teachers, Child Nutrition Personnel, Federal Programs Coordinator	
CNP status	Superintendent, Principal, Counselor, Asst. Principal, Student, Parent, Testing Coordinator, CNP Coordinator and staff, Technology Coordinator, Immediate Teacher, Federal Programs Coordinator	No
EL Status	Superintendent, Principal, Counselor, Asst. Principal, Teachers, Student, Parent, Testing Coordinator, Technology Coordinator, EL Supervisor, Assigned Teachers, After School Care Personnel, Child Nutrition Personnel, Federal Programs Coordinator	No
Special Ed. Status	Superintendent, Principal, Counselor, Asst. Principal, Testing Coordinator, Special Ed. Coordinator, Assigned Teachers, After School personnel, Technology Coordinator, Federal Programs Coordinator	No
Medical Conditions	Superintendent, Principal, Asst. Principal, Nurse, Immediate Teacher, Lunch Room Personnel (if food allergy), counselor, bus driver, transportation supervisor and After School Personnel, if applicable	No
Grades/Test Scores	Superintendent, Principal, Counselor, Asst. Principal, Student, Parents or Legal Guardian, Gifted Teacher (only for assigned students), PST Committees, Appropriate Central Office Administrators, Testing Coordinator, Transfers to schools and Scholarship applications, C2C,	INOW Home Portal for parents and Teachers
Attendance	Superintendent, Principal, Assistant Principal, Attendance Clerks, Truancy Officers, Immediate Teachers, PST Committee, Counselors, Parents, Student	INOW Home Portal only
Discipline	Superintendent, Principal, Counselor, Asst. Principal, Technology Coordinator, WCBE Board Members (when applicable) and assigned teachers.	INOW Home Portal only

ALSDE may have full access for State Reporting Collection purposes.

Physical Security

This policy communicates the essential aspects of the WCBE physical security equipment and data storage in order to safeguard the integrity and availability of system resources and data.

- The WCBE will ensure computer systems and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss.

- The WCBE will ensure access is controlled to areas containing servers, data stores, and communications equipment. Access to secured areas are locked with limited key distribution. A record shall be maintained of all personnel who have authorized access.
- The WCBE will ensure that if a key is reported as missing, the lock will be changed or the lock will be re-keyed.
- The WCBE will ensure a log is maintained of all visitors granted entry into secured areas or areas containing sensitive or confidential data (e.g., data storage facilities). The visitor's name, organization, and the name of the person granting access shall be recorded. The visitor logs will be maintained for a period of two academic years.
- The WCBE will ensure all visitors are escorted by a person with authorized access to the secured area.
- The WCBE will ensure all facilities containing computer and communications equipment have an appropriate fire suppression system or extinguisher readily available and in working order.
- The WCBE will store equipment above the floor, in racks whenever feasible, or on a raised floor to prevent damage from dampness of flooding.
- The WCBE will monitor and control the removal of all data-storing IT equipment. A record of all such items entering or exiting their assigned location will be maintained.

Data Quality

- Job descriptions for employees whose responsibilities include entering, maintaining, or deleting data shall contain provisions addressing the need for accuracy, timeliness, confidentiality, and completeness. This includes, but is not limited to: counselors, special education staff, and CNP staff handling free and reduced lunch data.
- Teachers shall have the responsibility to enter grades accurately and in a timely manner.
- School administrators shall have the responsibility to enter discipline information accurately and in a timely manner.
- It is the responsibility of all administrators and/or supervisors to set expectations for data quality and to evaluate their staff's performance relative to these expectations annually.
- Supervisors should immediately report incidents where data quality does not meet standards to their superior and to any other relevant department, including the State Department of Education, if applicable.

Data Governance Training

<u>Administrators/Supervisors</u>

- Principals and central office supervisors will receive refresher training on FERPA and other data procedures annually at a principal's meeting.
- Principals and central office administrators shall contact the technology coordinator when in doubt about how to handle information.
- Principals and central office administrators will be kept aware of emerging issues pertaining to data security.

School Counselors

- School counselors will be trained and refreshed on FERPA and other data security procedures annually.
- School counselors' adherence to the data security procedures will be monitored by the technology department through random audits when needed.

Teachers and Staff

- All new teachers will complete training on District technology policies, including how their use of technology is governed by FERPA and other data security procedures established by the WCBE.
- All users will receive reminders throughout the year via email regarding malware threats and phishing scams and how to report suspected threats.

Parents and Community

- School administrators shall educate PTOs, boosters, and other parent groups about FERPA and student confidentiality annually.

Data Exchange to External Service Providers

Student directory information may be transferred to an external service provider, such as an online website that teachers wish students to use for educational purposes. Provide that:

- The teacher follows the protocols for getting approval for the site to be used.
- The district notifies parents about their rights to restrict their child's data from being shared with such sites. The rights shall be listed in the student handbook distributed annually.
- The transfer of data is handled in a manner approved by the technology department, or is performed by the technology department.

No FERPA protected educational records will be transferred to an external service provider without prior approval of the Data Governance committee. The only exception is the Alabama State Department of Education. Approvals will be handled in the following manner:

1. Requesting party completes the 3rd party provider form.
2. The form is submitted by the requesting party to the technology coordinator.
3. The technology coordinator convenes the Data Governance Committee.
4. The Data Governance Committee makes a determination.
5. The requesting party is notified of the decision within 30 days of the request.