Dothan City Schools

District Technology Plan

2025-2026

Dothan City Schools

District Technology Plan

2024-2025

Updated: October 15, 2025

Contents

1) Executive Summary

a) Description of the School District/School

Located in Southeast Alabama, Dothan City Schools serves more than 8,285 Pre-Kindergarten through 12th-grade students throughout Dothan, Alabama. 19 schools comprise the district, including 2 Pre-Kindergarten centers, 11 elementary schools including one special admission math and science school, one school that exclusively serves 6th grade, one middle school that serves grades 7-8, one 9th grade academy, one virtual school for grades 7-12, one high school that serves grades 10-12, and two program sites dedicated to specialty education: one for students receiving alternative education and a career-technical education facility for grades 10-12. Each program seeks to develop engaging and meaningful opportunities for students at the elementary, middle, and high school levels.

Kelly Springs Elementary, Beverlye Intermediate, Highlands Elementary, Heard Elementary, Selma Street Elementary, Girard Elementary, and Morris Slingluff Elementary serve our students in K through 5th grade using a variety of hands-on lessons to engage students in work that is challenging, adventurous, and meaningful. Jerry Lee Faine Elementary serves students in Pre-K through 5th grade while Hidden Lake Primary serves our K-2nd grade students.

Carver School for Math, Science, and Technology is the system's Math, Science, and Technology School and heavily emphasizes investigation and discovery and seeks to prepare students for STEM-related college and career pathways. It retains a competitive admission policy, where students are accepted based on test scores. Carver MST serves Grades 3-6.

Dothan 6th grade Center is our newest school that now exclusively houses our 6th Grade students from across the district. Their focus is on fostering a nurturing and collaborative atmosphere where students thrive. With a dedication to integrating real-life connections, offering enriching learning experiences that equip our students with the essential skills for success.

Our Secondary Schools develop a diverse pipeline of students prepared for rigorous high school coursework and promote Advanced Placement courses so that more Alabama graduates will be prepared for college, the workforce, and life. Dothan Preparatory Academy serves our grades 7th through 8th, Carver 9th Grade Academy serves our 9th grade and Dothan High School serves our 10th through 12th grade. Dothan Tech serves as the career and technical school for students attending Dothan High, offering students opportunities in Automotive Repair, Health Sciences, and more.

Dothan City Virtual School provides a flexible and engaging virtual learning experience for motivated, independent learners in grades 7-12. Students may also participate in specialized courses at Dothan Tech or other DCS schools.
First Class Pre-Kindergarten is offered through Dothan City Early Education Center for children zoned for DCS. Dothan City Head Start Center provides additional services to DCS.

Demographics

The percent of students receiving free and reduced lunches at each school is as follows: Beverly Intermediate School = 93%, Carver 9th Grade Academy= 73%, Carver School of Math, Science, and Technology= 63%, Dothan City Virtual School= 70%, Dothan High School= 67%, Dothan Preparatory Academy= 78%, Dothan City Early Education Center= 66%, Faine Elementary School= 96%, Dothan 6th Grade Center= 84%, Girard Elementary School= 97%, Head Start/Pre-K= 98%, Heard Elementary School= 77%, Hidden Lake Elementary School= 84%, Highlands Elementary School= 45%, Kelly Springs Elementary School= 80%, Selma Elementary School= 91%, and Slingluff Elementary School= 86%.

5.31% of students in the district that are identified as English Language Learners. 18.06% of the district's students are identified as needing special education services. Dothan City Schools has a Pre-School/Head Start Program that serves approximately 543 children spanning 29 classes between Dothan City Early Education Center and Dothan City Head Start Center.

The enrollment for Dothan City Schools has increased over the last five years. The enrollment for the 2025-2026 school year is 8,285 students which shows an increase from 7,891 students in 2020-2021. The average daily attendance for the school system is over 91%. The Dothan City Schools system employs 1,148 people. There are 664 certified employees and 484 support staff employees.

Located in the southeastern part of Alabama, Houston County is in the heart of the state's Wiregrass region, which produces one-fourth of the nation's peanuts, rightly earning it the title of Peanut Capital of the World. Houston County was created by an act of the Alabama State Legislature on February 9, 1903, making it the newest of Alabama's 67 counties. Dothan is the largest city in Houston County and has served as the county seat since 1903. Dothan is a growing city, with a 2023 population of 71,258, showing an increase from 71,072 in 2020. It is the 8th largest city in Alabama. Spanning over 90 square miles, Dothan has a population density of 793 people per square mile. The median household income in Dothan is $55,052, with a poverty rate of 19.2%. The median rental cost in recent years is $958 per month, and the median house value is $232,500. The racial composition of Dothan is 56.05% White, 33.42% Black or African American, 1.58% Asian, and 4.23% multiracial, while 4.41% of residents are Hispanic or Latino. The median age in Dothan is 40.4 years, 38.6 years for males, and 42.6 years for females. Educationally, 88.0% of residents aged 25 and older have a high school diploma, and 27.3% hold a bachelor’s degree or higher.

Dothan City Schools is ranked as one of the top employers in Houston County, ranking second just behind Southeast Health. Dothan offers a number of recreational opportunities to visitors. Citizens of Dothan and its visitors enjoy nationally recognized sports facilities such as Westgate Park, Westgate Softball Complex, Westgate Tennis Center, and Rotary Miracle Field. Dothan is home to the Future Masters' Golf Tournament and to the Robert Trent Jones Golf Trails' Highlands Oaks as well as the annual host to the Southern Regional Karate Championships. Landmark Park is a 100-acre living history farmstead circa 1890s that was typical to this area. Each Fall Dothan hosts the National Peanut Festival, paying tribute to the area's contribution to the peanut industry. There are a number of other attractions in downtown Dothan. The Wiregrass Museum of Art features rotating exhibits of regional and national artists as well as a classroom/studio and a children's hands-on gallery. The downtown area offers motorists a pictorial history of the town through a number of colorful murals on various city buildings. The Dothan Opera House is an impressive Neoclassical Revival structure that dates from 1915. The Mule Marker in Poplar Head Park pays tribute to the animal that played a major role in the Wiregrass region's early development. Dothan City Schools has partnered with Wiregrass Foundation, a grassroots community group, to develop a co-owned strategic plan for excellence in education. Education is a shared responsibility among students, parents, schools, and the community. This reform effort seeks to unite all stakeholders in the common goal of transforming Dothan City Schools into institutions that prepare our youth for education after high school and for the world of work in the 21st century.

Notable Achievements and Areas of Improvement

Student achievement for students enrolled in Dothan City Schools has consistently been comparable to Alabama state average proficiency in Reading, Math, and Science as evidenced in the two-state assessments, ACAP (Alabama Comprehensive Assessment Program). While enrollment has fluctuated within the three years, our students have maintained proficiency levels comparable to state averages and have adapted to remote/virtual learning utilizing various online platforms to support teaching and learning. Disaggregated data among the reporting subgroups reflect that there are significant gaps that are consistent within the three-year period. However, these gaps have narrowed over the past three-year period. As our instructional teams review the data and conduct needs assessments, we note that to truly reflect student knowledge, more training for students in the use of technology, particularly at the lower grade levels, needs to be addressed. Therefore, moving forward, the team members initiated a phased approach to addressing the following needs:

- to focus attention and implementation on equal access to devices and the internet; every classroom (interdisciplinary) addressing technical vocabulary; high-quality instruction and professional development in the form of a blended approach instructional model i.e., asynchronous and synchronous; ongoing communication plan with parents and stakeholders in utilizing digital resources.
- to monitor and manage ongoing online tutorial sessions created as professional development for educators.

b) District Vision and Mission Statement

i) Mission Statement

(1) C.A.R.E.S. "Communicate, Achieve, Relate, Engage, Succeed"

ii) Vision Statement

(1) EMPOWER EVERYONE EVERYDAY

c) Additional Information

Our Health Services, as well as our Mental Health community leaders, have developed a school-based mental health program that provides on-site mental health service including preventative and crisis intervention. The Alabama Department of Mental Health and the Alabama Department of Education have identified the need for a greater integration of mental health services in public schools. There is an increasing concern about the growing number of children and adolescents who experience difficulties associated with the adverse effects of social and emotional disturbance. In school-age children and adolescents, unmet mental health needs can cause negative and oftentimes tragic long-term consequences. Those may include dropping out of school, substance abuse, a lack of vocational success, and an inability to live and function independently. Individual student records are confidential and information is not shared with school staff without parental consent. All services will be provided in a quiet, private, and confidential space in each school. Neither students nor parents will be billed for care.

2) Stakeholder Involvement

Our stakeholders were key administrative staff at the district level. Input was gathered electronically from the Curriculum Department, Health Services, Auxiliary Services, Special Education, ELL, Testing, Career Tech, Federal Programs, and Technology. The principals selected their respective representatives. These representatives communicated and worked collectively as needed on school technology plans. They referred to the district plan to help formulate their school plans.

The stakeholders included Jeremy Green (Director of Technology Services), Blair Peterman (Health Services), Sarahann Odom (ELL), Alyssa Dyre (Director of Special Education), Sherry Corbitt (Director of Instructional Services), Ryan Richards (CTE Director), Patrick Mallory (Chief Operations Officer/HR Director), and Lee Jacobs (Assistant Superintendent-Director of the Division of Accountability/Federal Programs) to assemble the district technology plan. Each stakeholder was given the authority and responsibility to collaborate and provide input on a plan that we could attain and sustain.

The final District technology improvement plan will be assembled for reference by the individual school plans. The finalization of the school plans will take place after stakeholders refer to the district plan to ensure compliance and completeness. The final District plan will be emailed and posted electronically for review by all stakeholders.

3) Data Sources & Funding Sources

a) Data Sources

- Compliance Monitoring Reports
- Continuous Improvement Plan
- Discipline and Attendance Reports
- Graduation Rates
- Inventory & Infrastructure Report - Fast and Easy Access to Network, and Availability of Technology
- Technology Program Audit, Etc.
- Alabama Educator Technology Survey

b) Funding Sources

- Capital Improvement Fund
- Career Technical Funds
- General Fund
- Perkins
- Title I, Schoolwide
- Title III
- USAC Technology
- IDEA Funding (Federal)

4) Needs Assessment

a) Technology Infrastructure - WAN, LAN, wireless access points, network switches, etc.

i) Needs

- We need to implement a comprehensive network equipment management system to enable proactive monitoring, timely response, and effective recovery from equipment failures or operational issues.
- We need to upgrade all network switches, wireless access points, and battery backups located in the district data center and in each school's MDF/IDF. Many of these devices are approaching end-of-support status. The new equipment should be integrated into a unified management platform to ensure centralized configuration management, automated backups, streamlined firmware updates, and improved monitoring of potential issues.

ii) Strengths

- The district has implemented robust security systems, including Endpoint Detection and Response (EDR) on all production server systems, centralized application patch management, and Syslog platforms. These tools provide both proactive and reactive responses to security events across servers and workstations. Multi-Factor Authentication (MFA) is enforced for all user email accounts, with an additional MFA layer applied to administrative and privileged accounts for enhanced protection.
- A comprehensive backup and disaster recovery strategy is in place, utilizing both Grandfather-Father-Child and 3-2-1-1-0 backup methodologies. Data is replicated across multiple secure locations, ensuring redundancy, integrity, and rapid recovery in the event of a disaster or data loss.
- Next-Generation Firewalls are deployed at all campuses, the district data center, and the network core. These devices provide advanced protection through dynamic, user- and device-based content filtering and granular access control, helping safeguard critical infrastructure and maintain compliance with district security policies.
- Our district's internet bandwidth has been upgraded to meet the growing demands of a technology-driven educational environment. In addition, WAN bandwidth has been expanded at high device-density locations—Carver 9th Grade Academy, Dothan Preparatory Academy, and Dothan High School—to support continued growth in instructional and administrative technology use.

These strengths and needs were identified by school walk-through, feedback from users and administration, security audits, and inventory reports

b) Technology Inventory - fast and easy access to technology

i) Inventory Strengths

- All student Chromebooks have been refreshed within the last year, and schools continue to expand device availability at the K–6 grade levels. Each school also maintains an ongoing replacement cycle to address damaged or outdated devices, ensuring that all students have access to reliable, up-to-date technology that supports seamless instruction and learning.
- All Windows and Chrome devices in our district are monitored to ensure that they receive the most recent security updates, application updates, malicious activity, and performance through Microsoft SCCM, Google Workspace Admin Console, and Sophos Central Security.

ii) Inventory Needs

- We need to integrate our desktop, laptop, and network infrastructure inventory into the technology department's existing system. Currently, we maintain a separate inventory for these capital fixed assets, but by consolidating all devices—including Chromebooks—we can store comprehensive information on each device. This will enable granular reporting and improve our planning processes.
- Our district is in need of an automated reporting system to support the 5-year device refresh lifecycle. This system will assist district and school administrators in planning by identifying which devices need to be upgraded each year, ensuring that all devices remain current and fully functional. This proactive approach will improve the management of technology assets and prevent disruptions in the learning environment due to outdated equipment.
- We need to upgrade all network switches, wireless access points, and battery backups located in the district data center and in each school’s MDF/IDF. Many of these devices are approaching end-of-support status and will soon no longer receive manufacturer updates or replacement parts. Since most student devices rely on Wi-Fi connectivity, maintaining a fully operational and secure wireless network is critical to instructional success.

These strengths and needs were identified by school walk-throughs, surveys, and inventory reports.

c) Student Learning - subject area processes and content; 21st C. skills and dispositions to ensure school, career, and life success

i) Needs

- In-house or State developed technology training for grades K-8 with the corresponding rubric
- More concept-oriented technology training instead of keystroke-oriented teaching to prepare for changes in technology, along with hands-on, small-group instruction
- More technology application and integration into the core curriculum

ii) Strengths

- Students are consistently challenged and encouraged to utilize technology to complete assignments within course standards. Students are assigned online learning paths based on their benchmark assessment results.
- Our technology training addresses life skills and CCRS standards.
- Edgenuity and ACCESS online curriculum as well as other district-wide applications are being used across secondary grade levels for remediation, acceleration, and to create individual learning paths for students to use attending class in the traditional brick-and-mortar setting or virtually.

These strengths and needs were identified by surveys and tech program audits.

d) Professional Learning Program - Teachers, Staff, & Leaders

i) Needs

- More technology PD for administrators so they can make wiser purchasing decisions and better evaluate technology usage.
- Implement a training system to train new and existing employees on effectively using technology resources available to them.

ii) Strengths

- District funds are used for professional development to meet standards-based instruction.
- We have used a collaboration product for delivery of PD throughout the District.
- Principals are being encouraged to use the train-the-trainer model for their staff.

These strengths and needs were identified by surveys.

e) Teacher - Teaching - how teachers use technology to teach as well as require students to use technology to learn

i) Needs

- More collaboration between classrooms that extend beyond building borders to emulate the business world.
- More use of State & locally provided resources such as ALEX, ACCESS, & AVL.
- The guided responsible use of AI platforms integrated into everyday curriculum to help prepare students for college or the workforce.

ii) Strengths

- Interactive flat panels installed in every classroom in the district.
- Teachers and students are encouraged to use Web 2.0 collaboration tools like Google Docs, sheets, etc.

These strengths and needs were identified by surveys.

f) Teacher - Productivity - how teachers use technology for increased productivity

i) Needs

- Need teachers to embrace and nurture an environment that supports innovative uses of technology.
- Teachers meet local, State, and national technology standards.
- Teachers appropriately and regularly assign learning activities that integrate the use of technology tools.

ii) Strengths

- Teachers use technology to gather and analyze data for improving student achievement.
- Educators will foster and nurture an environment that supports innovative uses of technology.
- Teachers are actively supporting technology PD to enhance their productivity.

These strengths and needs were identified by surveys.

g) School Leaders - Productivity - administrators use of technology for increased productivity

i) Needs

- Administrators meet local, state, and national standards for technology integration.
- More technology PD for administrative staff.
- Administrators use a variety of evaluation data to make decisions related to technology.

ii) Strengths

- Administrators use technology regularly to gather and analyze data to assess instructional effectiveness
- Administrators use technology to communicate with stakeholders at the local, District, and State levels.
- Administrators are mandating the use of technology tools within their authority

These strengths and needs were identified by surveys.

5) Professional Learning

We encourage the "train-the-trainer" approach in our District for professional development. We try to use face-to-face onsite training, when possible, with a variety of trainers including in-house staff, vendors, and third-party trainers when necessary. Administrators are encouraged to participate in technology training to help them evaluate the effectiveness of teachers using technology. Teachers are encouraged to aid in technology integration with a focus on classroom use of Chromebooks in grades K-12.

6) Inventory

a) 2025-2026 District Technology Inventory.

i) I certify that I have attached the Technology LEA Inventory.

7) Infrastructure

a) WAN Infrastructure.

All network-connected devices are centrally managed and secured with password protection. The district provides a 1.5 Gbps fiber connection from the Central Office data center to its three largest and highest device-density campuses—Carver 9th Grade Academy, Dothan Preparatory Academy, and Dothan High School—and a 1 Gbps fiber connection to all other schools. All network traffic from these locations is aggregated through a 10 Gbps trunk link into the Central Office data center, ensuring reliable, high-speed connectivity across the district.

b) LAN Infrastructure.

We use enterprise-grade managed switches throughout our District including all remote locations both instructional and non-instructional facilities. We provide a 1Gbps connectivity to all computers through copper and/or fiber connections within the schools. We have over 35 virtual servers at the Central Office providing centralized access to the Internet, email, student information systems, and common classroom and clerical applications.

c) Connectivity and Bandwidth.

The Central Office is connected to all schools by a 10Gbps fiber-optics backbone with a 1Gbps fiber link to each school. All non-instructional facilities are also connected by 1Gbps lines to a central communications network that connects to the Central Office by fiber-optic cable to handle the combined loads.

d) Internet Access

DCS uses Alabama Super Computer Authority as our Internet Service Provider and is connected to them by way of a 2.5Gbps line from our Central Office which was upgraded from our previous 1.5Gbps connection.

e) Information Security & Safety

The district connects to its Internet Service Provider, the Alabama Supercomputer Authority (ASA), through an enterprise-grade next-generation firewall using a 2.5 Gbps fiber link. In addition to providing internet connectivity, ASA serves as the district's Security Operations Center (SOC), monitoring all inbound and outbound traffic for potential threats and intrusions.

To further enhance network security, the district utilizes an additional enterprise-grade next-generation inline security appliance that monitors multiple network protocols, blocks inappropriate or malicious internet activity, and provides granular web and application filtering controls for both students and staff. Each school and remote location also has its own next-generation firewall in place, ensuring that any security incident or infection is contained and isolated to that specific site.

The network infrastructure is built on managed, password-protected switches, providing secure and reliable internal connectivity. Sophos Intercept X Advanced is deployed across all servers and endpoints to protect against malware, ransomware, and other cyber threats, with centralized management for real-time visibility and response. This solution also identifies any unprotected devices that connect to the network. No desktop computers or servers are publicly accessible from the internet, maintaining a strong security posture districtwide.

f) Digital Content

While the district does not operate under a traditional 1:1 device assignment model (with the exception of Dothan City Virtual School), each classroom is equipped with enough Chromebooks to accommodate all students during instruction. The district serves over 8,500 students and maintains a fleet of more than 10,000 Chromebooks. Devices are stored in classroom charging carts and are available for use as needed, ensuring equitable access to technology for all students. Classrooms, labs, and media centers are equipped with computers offering access to a range of applications, including word processing, spreadsheets, databases, presentation tools, and internet access. The Alabama Virtual Library (AVL) is also available from these locations.

Networked educational tools such as Advanced Learning System, Imagine Learning Platform, and Pearson Learning are widely used. The Imagine Learning Platform and Advanced Learning System are specifically utilized for remediation and credit recovery in secondary schools.
The district is focused on adopting browser-based applications, including Book Systems Atrium for library management and Renaissance Place, which features Accelerated Reader. Some elementary and middle school students also have access to online keyboarding and technology application training. All secondary students are provided with secure logins, passwords, and network storage accessible from any district computer.

Our ongoing goal is to centralize applications, ensuring students can access resources from any device, anywhere. This approach accommodates students who transfer within the district, home-bound students, and those relocated for disciplinary reasons, ensuring equal access to resources for all.

8) Data Compliance

a) Data Governance Policy

I certify that I have attached a copy of the policy.

b) Acceptable Use Policy

I certify that I have attached a copy of the policy.

c) Data Governance Procedure

I certify that I have attached a copy of the procedures.

9) Alabama Technology Plan Goals and Activities

a) Alabama Technology Plan Goals and Activities

I certify that I have attached the Alabama Technology Plan Goals and Activities sheet.

10)Attachments

Attachment Name	Description	Associated Item(s)
DCS District Technology Inventory 25-26.pdf	District Technology Inventory *(page 17)*	4. a 4. b 6. a 7. a
DCS Data Governance Policy.pdf	Data Governance Policy *(page 19)*	8. a
DCS Acceptable Use Policy.pdf	Acceptable Use Policy *(page 22)*	8. b
DCS Data Governance Procedures.pdf	Data Governance Procedure *(page 32)*	8. c
DCS Strategic Plan 22-26.pdf	Goals and Objectives *(page 61)*	9. a

Dothan City Schools

District Technology Inventory

Tech Inventory 2025-
Dothan City

Submitted w/ 0 remainining blanks
You already Submitted all results to the ALSDE

edtech EDUCATIONAL TECHNOLOGY

		Section Internet WA2							Section 2 Personnel																			Section 2I* Devices				
Edit *orm	Internet	2 Internet &andwidth	WA2 EUuality		6 Lowest WA2	6 Highest WA2	Core WA2		2 Person nel	2 2 TC	2 Asst TC	2 Network Admin	2 5 Data Admin	2 6 Data Entry	2 Technicia n	2 Coach	2 Cybersecu rity	2 0 PS Admin	2 Other	2 2 Tech &oles	2 2 Asst Tech Coordinator	2 Other	2 Networ k	2 Data Admin	2 Data Entry Clerk	2 Technicia n	2 Tech Coach /	2 Cybersecurit y Specialist	2 PS Admin	Windows Other	Apple EOL	2 Chromebooks		
Submitted	AL Supercomputer Authority	2500	Other	No	1 GB	1.5GB	10GB	No	23	1	0	1	0	0	4	0	1	1	15	0	State Tech. Local	N/A	Local, Grant	Local	N/A	Local	N/A	Local, Grant	Local	320	0	211	0	0

		Section Instructional Gooms							Section 2 Shared Devices					Section Student Dedicated Devices Student Dedicated Device OS +rade Level															Section *aculty StaJJ Dedicated Devices Dedicated StaJJ Devices 2					
Edit *orms	District - School	2 Gooms	2 /w Wireless	Wireless	6 Personal Devices	+uest Wi-*i	2 Window s	2 2 Apple device	2 Chrome books	2 Other devices	2 5 EOL devices	/	st	2nd	rd	th	5th	6th	th	th	th	0th	th	2th	2 Student dedicated	Spare devices	EOL student	Admin ClassJied	CertiJied	Admin ClassJied	CertiJied	
Submitted	Dothan City - Beverlye IS	35	35	Excellent	35	2	No	Only at	57	0	362	0	0	None	None	None	None	None	None	None	None	None	None	None	None	0	0	0	Desktop, Laptop,	Desktop, Laptop	Desktop	2	27	10
							spe cified																						Smartphone					
							times																											
Submitted	Dothan City - Carver 8th Grade	32	32	Excellent	32	2	No	Only at	88	0	808	24	0	None	None	None	None	None	None	None	None	None	None	None	None	5	5	0	Laptop,	Laptop	Laptop,	4	18	
							spe cified																						Smartphone		Smartphone			
							times																											
Submitted	Dothan City - Carver Sch for Math and Tech	25	25	Excellent	25	1	No	Only at	0	0	596	0	10	None	None	None	None	None	Chrome	None	None	None	None	None	None	1	0	0	Desktop, Laptop,	Desktop, Laptop	Desktop, Laptop	5	50	5
							spe cified																						Smartphone					
							times																											
Submitted	Dothan City - Dothan HS	71	71	Excellent	71	1	No	Only at	41	0	1405	0	0	None	None	None	None	None	None	None	None	None	None	None	None	0	0	0	Desktop, Laptop,	Desktop, Laptop,	Desktop, Laptop,	16	167	28
							spe cified																						ChromeFook,	ChromeFook	ChromeFook			
							times																						Smartphone					
Submitted	Dothan City - Dothan Prep ACAD	60	60	Excellent	60	2	No	Only at	0	0	1095	0	50	None	None	None	None	None	None	None	None	None	None	None	None	0	0	0	Desktop, Laptop,	Desktop, Laptop,	Desktop, Laptop,	15	80	10
							spe cified																						TaFlet,	TaFlet,	ChromeFook			
							times																						Smartphone	ChromeFook				
Submitted	Dothan City - Early Ed Center	16	16	Excellent	16	1	No	Only at	0	0	19	0	0	None	None	None	None	None	None	None	None	None	None	None	None	0	0	0	Desktop, Laptop,	Laptop, TaFlet,	TaFlet,	3	48	32
							spe cified																						Smartphone	ChromeFook	ChromeFook			
							times																											
Submitted	Dothan City - Girard IS	37	37	Excellent	37	2	No	Only at	69	0	769	0	132	None	None	None	None	None	None	Chrome	None	None	None	None	None	0	0	0	Desktop, Laptop,	Desktop, Laptop	Desktop	7	65	4
							spe cified																						Smartphone					
							times																											
Submitted	Dothan City - Girard Primary Sch	31	31	Excellent	31	1	No	Only at	1	0	529	0	124	None	None	None	None	None	None	None	None	None	None	None	None	0	40	100	Desktop, Laptop,	Desktop, Laptop	Desktop, Laptop	5	32	6
							spe cified																						Smartphone					
							times																											
Submitted	Dothan City - Heard ES	25	25	Good	25	1	No	Only at	0	0	430	0	60	None	None	None	None	None	None	None	None	None	None	None	None	0	10	2	Desktop, Laptop,	Desktop, Laptop	Desktop, Laptop	6	25	5
							spe cified																						Smartphone					
							times																											
Submitted	Dothan City - Hidden Lake Primary	34	34	Excellent	34	2	No	Only at	28	0	505	0	54	None	None	None	None	None	None	None	None	None	None	None	None	0	0	0	Desktop, Laptop,	Desktop, Laptop	Desktop,	4	64	8
							spe cified																						Smartphone		ChromeFook			
							times																											
Submitted	Dothan City - Highland ES	39	39	Excellent	39	1	No	Only at	0	0	574	37	43	None	None	None	None	None	None	None	None	None	None	None	None	0	0	0	Desktop, Laptop,	Desktop, Laptop,	Desktop, Laptop	6	70	10
							spe cified																						Smartphone	Other				
							times																											
Submitted	Dothan City - Jerry Lee Paine ES	29	29	Excellent	29	2	No	Only at	0	0	584	0	54	None	None	None	None	None	None	None	None	None	None	None	None	0	0	0	Desktop, Laptop,	Desktop, Laptop,	Desktop	10	41	10
							spe cified																						TaFlet,	ChromeFook				
							times																						ChromeFook,					
																													Smartphone					
Submitted	Dothan City - Kelly Springs ES	43	43	Excellent	43	1	No	Only at	77	0	468	0	6	None	None	None	None	None	Chrome	None	None	None	None	None	None	2	0	0	Desktop, Laptop,	Desktop, Laptop,	Desktop, Laptop	6	84	11
							spe cified																						Smartphone	Smartphone				
							times																											
Submitted	Dothan City - Morris Slingluff ES	26	26	Excellent	26	1	No	Only at	92	0	400	0	0	None	None	None	None	None	None	None	None	None	None	None	None	0	0	0	Desktop, Laptop,	Desktop, Laptop	Desktop	9	5	6
							spe cified																						Smartphone					
							times																											
Submitted	Dothan City - Pre-SchHead Start	18	18	Excellent	18	2	No	Only at	112	0	54	0	0	None	None	None	None	None	None	None	None	None	None	None	None	0	0	0	Desktop, Laptop,	Desktop, Laptop	Desktop, Laptop,	6	12	72
							spe cified																						Smartphone		TaFlet			
							times																											
Submitted	Dothan City - Selma SES	37	37	Good	34	2	No	Only at	67	0	450	0	265	None	None	None	None	None	None	None	None	None	None	None	None	0	0	0	Desktop, Laptop,	Desktop, Laptop	Desktop	4	66	6
							spe cified																						Smartphone					
							times																											
Submitted	Dothan City - Virtual Sch	5	5	Excellent	5	4	No	Only at	38	0	419	0	0	None	None	None	None	None	None	None	None	None	None	None	None	419	0	0	Desktop, Laptop,	Desktop, Laptop	Desktop, Laptop	6	28	5
							spe cified																						Smartphone					
							times																											

Dothan City Schools

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.

G. 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)

H. 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.

Dothan City Schools

Acceptable Use Policy

INTRODUCTION:

Electronic instructional materials are selected by Dothan City School System to implement, enrich, and support the educational program for students. These materials must serve both the breadth of the curriculum and the needs and interests of individual students and employees. To this end, policies must be in place to assure the selection of materials of the highest quality and appropriateness. The policies contained within this document are to serve as legal and acceptable use of the Dothan City Schools network (DCSNet), as well as, copyright and acceptable use of video and software within the classroom environment.

DCSNet Acceptable Use Policy establishes policies and guidelines for the use of Internet and the Dothan City School System's wide area network for students and Dothan City School System's employees. The use of this electronic resource is a privilege not a right. Failure to adhere to the policy will result in the revocation of the user's access privilege. At school, student access to the DCSNet and the use of the Internet will be under teacher direction and will be monitored as any other classroom activity.

We recognize that the use of technology always requires attempts to balance the benefits against the possibilities of danger, security problems, and abuse. Rapid changes in technology and growth in the range of content available makes this a constant challenge. Thus, it is the intention of Dothan City Schools that all technology resources will be used in accordance with any and all school system policies and procedures as well as local, state, and federal laws and/or guidelines governing the usage of technology and its component parts. Additionally, it is implied that all students and employees of Dothan City Schools will use the provided technology resources so as not to waste them, abuse them, interfere with or cause harm to other individuals, institutions, or companies.

- The administrators of each school will be responsible for establishing specific practices to enforce this policy at individual schools.

- All Dothan City School students and employees shall review and adhere to this policy for access to the DCSNet. Employees shall sign, and return the Dothan City Schools DCSNet and Internet Application and Contract to the DCS Personnel Department. Students and guardians of students must sign and return the Dothan City Schools Student Internet And/Or Email Permission Form for Internet and/or email use within Dothan City Schools.

- Highlights of this policy will be prominently displayed in all computer labs and posted on the Dothan City Schools district technology webpage.

- All Dothan City Schools technology resources, regardless of purchase date, location, or fund, are subject to this policy as well as the purchasing and disposal guidelines set forth by the Dothan City Schools accounting department.

- Some of these policies pertain to technology equipment personally owned by school employees and students and brought into school facilities. All personal technologies used on any Dothan City School campus are subject to this policy and may be used only if such usage is in compliance with all school system policies, procedures, and guidelines as well as local, state, and federal laws.

- All electronic content stored on any external storage medium or personal off-site storage location that is brought to or accessed from a Dothan City Schools campus is subject to all school system policies and guidelines as well as local, state, and federal laws.

- Any questions about this policy, its interpretation, or specific circumstances shall be directed to the Director of Technology Services (DTS) before proceeding.

- Violations of this policy will be handled in a manner consistent with the Dothan City Schools Code of Conduct and/or Dothan City Schools Personnel Policy Manual.
- Each school will name a SYSop. The SYSop will assist with the enforcing of this policy.

I. LIMITATION OF LIABILITY:

A. The Dothan City School System makes no guarantee that the functions of the services provided by or through DCSNet will be error-free or without defect.

B. The Dothan City School System will not be responsible or liable for:

- any damage suffered, including but not limited to, loss data or interruptions of service
- the accuracy or quality of the information obtained through or stored on the system
- financial obligations arising through the unauthorized use of the system
- any information collected or disseminated through DCSNet by any un-authorized individual(s)

II. ACCESS:

A. The use of all Dothan City Schools technology resources is a privilege, not a right, and inappropriate or suspected inappropriate use will result in a cancellation of those privileges pending investigation. Moreover, users of Dothan City Schools technology must be aware that Dothan City Schools cannot assume any liability arising out of the illegal or inappropriate use of technology resources.

B. Users should not have any expectation that their usage of such resources is private. Reasonable efforts will be taken to maintain security of technology resources, but Dothan City Schools cannot ensure that such security will not be penetrated or breached, and cannot assume any liability arising out of any such penetration or breach of security.

C. Users should not purchase or dispose of software, hardware, peripherals, or other technology related devices without consulting the technology staff. All personnel should adhere to the purchasing and disposal guidelines set forth by the Dothan City Schools accounting department when purchasing or disposing of technology items.

D. Individuals may use only accounts, files, software, and/or other technology resources that are assigned to, provided to, or approved for him/her.

E. Individuals may not attempt to log in to the network using any network account and/or password other than the login(s) assigned to him/her or allow someone to use his/her network account and/or password to access the network, email, or the Internet.

F. Individuals must take all reasonable precautions to prevent unauthorized access to accounts and data and any other unauthorized usage within and outside Dothan City Schools. Any such unauthorized usage shall be reported immediately to the school principal and/or the DTS.

G. Individuals identified as a security risk may be denied access.

H. Any use of technology resources that reduces the efficiency of use for others will be considered a violation of this policy.

I. Individuals must not attempt to disrupt any computer services or data by engaging in activities including, without limitation, spreading viruses, spamming, excess network and/or Internet activity, or modification of equipment or infrastructure.

J. Individuals must not attempt to modify technology resources, utilities, and configurations, or change the restrictions associated with his/her accounts, or attempt to breach any technology resources security system or filtering system, either with or without malicious intent.

K. Personal technology related devices such as but not limited to laptops, PDAs, smartphones, iPods, etc. used on school grounds are subject to all items covered in this policy and should not access local area network or wide area network resources without the explicit permission of the technology staff. Public Internet access is available for visiting devices and is subject to the conditions outlined in this policy and all other school system policies and guidelines as well as local, state, and federal laws.

L. The DTS and/or school system administrators will determine when inappropriate use has occurred and they have the right to deny, revoke, or suspend specific user accounts.

M. No network device such as a switch, hub, router, access point or print server shall be allowed on the DCSNet unless provided or approved by the Technology Services staff.

III. PRIVACY:

A. To maintain network integrity and to insure that the network is being used responsibly, the DTS and/or other designated technology staff reserve the right to inspect any and all data,

including data stored by individual users on individual school or personal devices. Users should be aware that activities may be monitored at any time, without notice.

B. Users should not have any expectation that their use of technology resources, including files stored by them on the DCSNet, will be private and will be secure from access by others. Reasonable steps will be taken to maintain the security of technology resources, but no assurance can be given that penetration of such security will not occur.

C. Because communications on the Internet are, often, public in nature, all users should be careful to maintain appropriate and responsible communications.

D. Dothan City Schools cannot guarantee the privacy, security, or confidentiality of any information sent or received, either via the Internet, an email facility, telephone, or otherwise.

E. Users are encouraged to avoid storing personal and/or private information on the district and/or schools' technology resources.

F. The system-wide technology staff does perform routine backups in an effort to assure continuity of business. There can be no assurance, however, that technology resources will be available within a particular time frame following an outage and, in particular, that information that existed prior to an outage or malfunction, or that existed prior to a deliberate or inadvertent deletion, can be recovered. Users are responsible, without limitation, for the maintenance and backup of critical files and/or data.

G. Reasonable steps and procedures will be taken to secure student records, media center collections and accounting information. Such information shall be backed up in a routine manner.

IV. COPYRIGHT:

A. Illegal copies of software may not be created or used on school equipment.

B. Any questions about copyright provisions should be directed to the DTS.

C. Aspects involving the legal and ethical practices of appropriate use of technology resources will be taught to all students and employees in the system (i.e. as part of the Technology Education Curriculum, during lab orientation, network orientation, faculty meetings, etc). There can be no assurance as to the

extent and effectiveness of such training. Again, all questions regarding legal and ethical practices of appropriate use should be directed to the DTS.

D. Copyright is implied for all information (text, data, and graphics) published on the Internet. Web page authors will be held responsible for the contents of their pages. Do not "borrow" icons, sounds, or graphics from other pages without documented permission. It is the user's responsibility to secure proper usage permission.

E. Duplication of any copyrighted software is prohibited unless specifically allowed for in the license agreement and then, should occur only under the supervision and direction of the Technology staff.

F. A backup copy of all purchased software programs should be made and, thus, become the working copy.

G. All original copies of software programs, including those purchased with departmental funds, will be stored in a secure place.

H. For security and insurance purposes, the local SYSop, technology aides, and/or the district level technology staff will be the only people with access to original software disks at a given school location with the exception of CD-ROMs required when accessing the program. System-wide software originals will be housed at the DTS office.

I. In almost every case, a single copy of a given software package is purchased; it may only be used on one computer at a time. Multiple loading or "loading the contents of one disk onto multiple computers," (1987 Statement on Software Copyright) is NOT allowed.

J. If more than one copy of a software package is needed, a site license, lab pack, network version, or Internet portal license must be purchased. The DTS and/or the person requesting the software will be responsible for determining how many copies should be purchased.

K. Either the DTS or respective school principal is authorized to sign license agreements for a school within the system. Copies of any system-wide license agreements must be signed by the DTS and/or Superintendent and distributed to all schools that will use the software.

L. The District technology staff is responsible for installation of all software in use on the wide area network, local area network and/or individual workstations/laptops within the Dothan City Schools. Technology lab aides or other designated staff may install software on local workstations with permission by the DTS.

M. Users are expected to be familiar with and adhere to the current Copyright and Fair Use Guidelines for Teachers posted on the Dothan City Schools web site.

V. EMAIL:

E-mail is considered in the same category as paper transmissions in the matter of public records. As defined in the Code of Alabama 1975, Section 36-12-2, e-mail is a public record when it is created by a Dothan City School System employee in the course of conducting school business, and when it documents the activities and business of school employees. These emails shall include any messages, calendars and attachments as public record. Student created e-mail is not considered a public record. All student created e-mail, including messages, calendars and attachments may be reviewed by supervising teacher, principal or administrator.

A. Dothan City Schools provides access to email for all employees; upon request, generic accounts for employee sponsored organizations and classes; and on a limited basis, with teacher or principal recommendation and written guardian permission, for secondary students.

B. Technical support is provided for Dothan City Schools email accounts used to conduct educational and/or instructional business.

C. Personal use of email is permitted as long as it does not violate Dothan City Schools policy and/or adversely affect others or the speed of the network. Employees should use their Dothan City Schools email account for all school related email correspondence.

D. When employing email, all employees are responsible for maintaining professionalism at all times. Email communication sometimes lends itself to impulsive and to informal communication. Employees must be constantly mindful of the need to carefully review and reconsider email communications before responding to and/or sending email. Dothan City Schools email accounts may not be used for political activity, personal gain, commercial purposes, or profit.

F. Dothan City Schools email accounts may not be used for attempting to send or sending anonymous messages.

G. Dothan City Schools email accounts may not be used for sending mass emails unless to parent lists or other for educational purposes.

H. Dothan City Schools email accounts may not be used for posting or forwarding other user's personal communication without the author's consent.

I. Because e-mail is not necessarily securely transmitted, discretion must be used when sending, or encouraging the receipt of email containing sensitive information about students, families, school system employees, or any individuals. There can be no assurance that email will be confidential and/or private.

J. Dothan City Schools make a reasonable effort to maintain (backup) email for normal business operations. Backups are maintained for a maximum of 13 days. Deleted email is purged every 7 days.

K. Users required to maintain email for an extended period, for public record, or email in excess of the user’s email quota must print said emails. The technology staff, Dothan City Schools administrative staff, or the Dothan City Board of Education does not support or advocate the use of email archives.

L. Incoming and outgoing email is filtered by the District for inappropriate content. However, no filtering system is foolproof and material deemed inappropriate by individual users may be transmitted in spite of filtering.

M. Email records may be requested in accordance with the Dothan City Schools Board of Education policy: FIIe:BE.

VI. INTERNET USE:

A. The intent of the Dothan City Schools is to provide access to resources available via the Internet with the understanding that staff and students will access and use information that is appropriate for the various curricula.

B. All school rules and guidelines for appropriate technology usage as well as local, state, and federal laws apply to usage of the Internet.

C. Teachers should screen all Internet resources before projecting them in the classroom.

D. Students gain access to the Internet by agreeing to conduct themselves in a considerate and responsible manner and by providing written permission from their parent(s)/guardian(s).

E. Students are allowed to conduct independent research on the Internet upon the receipt of the

Dothan City Schools Student Internet And/Or Email Permission Form.

F. Permission is not transferable, and therefore, may not be shared. Existing permission forms are valid until new forms are received. Students are not required to have new forms signed when changing schools.

G. Students who are allowed independent access to the Internet have the capability of accessing material that has not been screened.

H. Internet activity can and will be monitored, along with other aspects of technology usage.

I. Internet access for all users is filtered, through one central point, by URL (web address) and by IP address and may be filtered by keyword. All Internet sites that may be considered harmful to students will be filtered.

J. URLs (web addresses) and IP addresses may be added to or deleted from the filtered list by the District Technology staff.

K. Staff members may request to review filtered categories. Users requesting sites for blocking or unblocking, must list specific URLs.

L. Successful or unsuccessful attempts to bypass the Internet filter by using proxies or other resources are a violation of this policy.

M. Users will not post or transmit any personal contact information about themselves or other people. Personal information includes: home and/or school address, work address, home and/or school phone numbers, full name, social security number, etc. Exceptions include college registrations, online tests and any other DCS approved use.

N. Users shall not agree to meet with anyone they have met on-line.

O. Users shall promptly disclose to his/her immediate supervisor such as teacher, principal, DTS or the network system administrator, any message received that is inappropriate or makes the user feel uncomfortable.

VII. WEB PUBLISHING:

A. The Dothan City Schools web site is limited to usage associated with activities of Dothan City Schools. The web site cannot be used for profit, for commercial purposes, to express personal opinions, or to editorialize.

B. The Technology Services staff and/or the Director of Information Systems reserves the right to reject all or part of a proposed and/or posted web page.

C. All pages posted on the Dothan City Schools web site must be designed and/or written with an approved editor.

D. Each Dothan City Schools webpage should clearly state the person responsible for the content.

E. All posted work must be of publishable quality with regard to spelling, usage, and mechanics.

F. All web page authors are responsible for the maintenance of their own pages.

G. All links should be checked regularly to make sure they are current and working. Pages that are not updated in a timely fashion; that contain inaccurate or inappropriate information; that violate copyright laws and/or that contain links which do not work will be removed; the author will be notified.

H. Unfinished pages should not be posted until they are fully functional.

I. A teacher's primary web page should be housed on the Dothan City School web site; however, the page may contain a link or links to teacher created web pages stored on a different commercial or private server. In this event, these pages should adhere to all Dothan City School policies as well as local, state, and federal laws.

J. Links from pages housed on the Dothan City Schools website to personal blogs, social networking sites, advertisements unrelated to school system business, and/or personal web pages are prohibited.

K. Pictures and other personally identifiable information should only be used with permission in writing from the parent/guardian of the student involved. No full names should be used, only first name, last initial. No written permission is required for in-school broadcasts (i.e. morning news, announcements, class profiles, etc.)

L. Student posting of personal information of any kind on the Dothan City School website or linking to personal information from the Dothan City School website is prohibited. Personal information includes: home and/or school address, work address, home and/or school phone numbers, full name, social security number, etc.

M. No written permission is required to list faculty/staff and their school contact information (phone extension, email address, etc.)

N. Permission for publishing employee photographs on the Dothan City School website is assumed unless the employee specifies otherwise in writing to their direct supervisor.

O. Infringement of copyright laws, obscene, harassing or threatening materials on web sites are against the law and are subject to prosecution.

VIII. AUDIOVISUAL:

A. Educators are permitted to use videos if (1) legitimate copies, not pirated copies are used, and

(2) videos are used as part of face-to-face instruction (teaching activities) by a teacher, and not for entertainment, reward or extra-curricular activities or behavior modification activities. A copy made of a video owned by another person or rented is not legal unless permission to make a copy is first secured from the copyright owner.

B. The use of a video in a school is considered public performance for which a license must be obtained. The use in direct instruction is the exception which provides "fair use" of videos in a school. If a school desires to use videos for these activities, public performance rights must be obtained. Video rental stores cannot grant this right.

C. An off-air recording can be made only when requested by a teacher.

D. A recording cannot be made and held until the subject matter is needed for instruction. A recording may be shown not more than two times within 10 days of the broadcast with the second showing only for instructional reinforcement. It may be kept 45 days before it has to be erased.

E. Students are not allowed to tape programs at home and bring them to school to be shown.

F. Cable network channels such as Disney, Discovery, or CNN, for example, cannot be recorded. There are exceptions for some programs of educational value which may be recorded. Permission information can be obtained from the cable networks or cable providers.

G. Teachers should keep in mind, at all times, the appropriateness of the content and the educational value of all audiovisual materials used in the classroom.

H. Each user of audiovisual media will adhere to the copyright law and this policy governing audiovisual use.

I. Rental videos shall not be shown.

J. Unauthorized copies of copyrighted videos shall not be made or used.

K. No audiovisual materials shall be shown without approval of the school principal. See the Dothan City Schools Audiovisual Evaluation and Request Form on the Dothan City School's web site.

L. Users are expected to be familiar with and adhere to the current Copyright and Fair Use Guidelines for Teachers posted on the Dothan City Schools web site.

IX. PARENTAL PERMISSIONS:

It is the responsibility of the staff posting information on the web, requesting videos, or designing publicity or public relations information to obtain written parental permission.

X. EXAMPLES OF INAPPROPRIATE USE OF RESOURCES:

The following are examples of inappropriate activities when using any Dothan City School network, email system, hardware, software, technology service, and/or Internet access:

A. Using another user's password or attempting to find out what another user's password is

B. Sharing your own password

C. Trespassing in another user's files, folders, home directory, or work

D. Saving information on ANY network drive or directory other than your personal home directory OR a teacher specified and approved location

E. Downloading, installing, or copying software of any kind onto a workstation, your home directory, or any network drive

F. Harassing, insulting, embarrassing, or attacking others via technology resources

G. Damaging technology resources including but not limited to printers, telephones, computers, computer systems, or computer networks (this includes changing workstation configurations such as screen savers, backgrounds, printers, BIOS information, preset passwords, etc.)

H. Intentionally wasting limited resources such as Internet bandwidth, disk space and printing capacity

I. Accessing inappropriate material from off-site storage locations and/or removable storage devices

J. Accessing inappropriate material from web sites or attempting to bypass the Internet filter to access web sites that have been blocked (sites containing information that is, for example, violent; illegal; satanic; sexual; demeaning; racist; inflammatory; and/or categorized as a social networking, blogging, or journaling, etc.)

K. Sending, displaying, or downloading offensive messages or pictures

L. Using obscene, racist, profane, discriminatory, threatening, or inflammatory language in a document, email, etc.

M. Using a digital camera, camera phone, or any other device capable of storing a still or video image to take inappropriate or embarrassing pictures without the subject's knowledge and/or consent

N. Excluding modifications made while working on an authorized school/school system publication or under the supervision of a teacher, editing/modifying digital pictures without the consent of the subject especially with the intent to embarrass, harass, or bully

O. Plagiarizing written words, pictures, music and/or other media types accessible through the DCSNet or the Internet

P. Using the DCSNet for commercial purposes or profit including offering, providing or purchasing products or services

Q. Using the DCSNet for political lobbying

R. Knowingly or recklessly posting or transmitting false or defamatory information about a person or organization.

Dothan City Schools

Data Governance Procedure

Applicable Laws and Standards
The District will abide by any law, statutory, regulatory, or contractual obligations affecting its information systems. The District's data governance policy and procedures are informed by the following laws, rules, and standards, among others:
FERPA
The Family Educational Rights and Privacy Act, applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students specific rights with respect to their data. (See Exhibit G.)
ALABAMA RECORDS DISPOSITION AUTHORITY
Alabama Law Section 41-13-23 authorized the Alabama Department of Archives and History to publish rules for Local Government Records Destruction. For more information:
http://www.archives.alabama.gov/officials/localrda.html.
ALABAMA OPEN RECORDS LAW

COPPA
The Children's Online Privacy Protection Act, regulates organizations that collect or store information about children under age 13. Parental permission is required to gather certain information; see www.coppa.org for details.
HIPAA
The Health Insurance Portability and Accountability Act, applies to organizations that transmit or store Protected Health Information (PII). It is a broad standard that was originally intended to combat waste, fraud, and abuse in health care delivery and health insurance, but is now used to measure and improve the security of health information as well.
Payment Card Industry Data Security Standard (PCI DSS)
This standard was created by a consortium of payment brands including American Express, Discover, MasterCard, and Visa. It covers the management of payment card data and is relevant for any organization that accepts credit card payments. See www.PCI security standards.org for more information.
ISO Standards (http://www.iso.org/iso/home/standards.htm)
ISO 17799:2000 – Information technology – Code of practice for information security management
ISO 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements
ISO 27002L2013 - Information technology – Security techniques – Code of practice for information security controls

PPRA

The Protection of Pupils Rights Amendment is a federal law passed in 1974 that bars the disclosure of personally identifiable data in student records to third parties without parental consent.

Data Governance Committee

Name	**Department**
Todd Weeks	Interim Superintendent
Todd Weeks, Director of Personnel	Personnel
Mike Manuel, Director of Finance	Accounting
Mark Williams, Technology Coordinator	Technology
Scott Faulk, Director of Secondary Curriculum	Student Services
Teresa Davis, Director of Primary Curriculum & Testing Supervisor	Testing & Student Services
Tonya Grier, Director of Child Nutrition Program	Child Nutrition
Carol Cunningham, Director of Exceptional Student Services	Exceptional Student Serv.
Jay Bruner, Director of Transportation & Student Safety	Transportation & Safety
Hunter Parrish, Senior Electronics Technician	Technology

Doretha James, Nursing Supervisor	Nursing
Katie Comeens	ESL
INOW Permission Committee	
Todd Weeks, Director of Personnel	Personnel
Mark Williams, Technology Coordinator	Technology
Kim Judy, INOW Administrator	Technology
Hunter Parrish, Senior Electronics Technician	Technology
Scott Faulk, Director of Secondary Curriculum	Student Services
Teresa Davis, Director of Primary Curriculum & Testing Data Supervisor	Testing & Student Services
Dr. Donnie Chambers, Principal	Principal

Data Security Measures

I. Data Classification

(A) Dothan City Schools System Data shall be classified into three major classifications as defined in this section. Requests for changes to the established data sensitivity classification or individual permissions shall be made to the Technology Department.

1) Class I – Public Use

This information is targeted for general public use. Examples include Internet website content for general viewing and press releases.

2) Class II – Internal Use

Non-Sensitive (See Class III) information not targeted for general public use.

3) Class III – Sensitive

This information is considered private and must be guarded from unauthorized disclosure; unauthorized exposure of this information could contribute to identity theft, financial fraud, breach of contract and/or legal specification, and/or violate State and/or Federal laws.

(B) FERPA Directory Information

Information disclosed as 'directory information' may fall into either Class I or Class II, depending on the purpose of the disclosure. The following is the District's list of directory student information:

- Student's name
- Address
- Telephone listing
- Electronic mail address
- Photograph
- Date and place of birth
- Major field of study
- Dates of attendance
- Grade level
- Participation in officially recognized activities and sports
- Weight and height of members of athletic teams
- Degrees, honors, and awards received
- The most recent educational agency or institution attended
- A student number assigned by the District (in some cases*)
- Homeroom

Data Classifications for Students

Student Data Classification

Student Data	Classification	Authorized Users	Web Access
Student Name*	Class I or II, depending on use	All, as needed	First Name, Last Initial only, except in press release, school newspaper, or C2C
District Student Number	Class II	Principal, Asst. Principal, Counselor, Registrar, Teachers, Student, Parent, CNP, Media Specialist, iNOW/Chalkable Data Manager. Also export to approved service providers in order to establish unique identities or accounts – requires Data Governance Committee approval.	No
State Student Number*	Class II	Principal, Asst. Principal, Counselor, Registrar Student, Parent, iNOW/Chalkable Data Manager.	No
Social Security Number*	Class III	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, iNOW/Chalkable Data Manager.	No
Home Phone Number	Class I or II, depending on use	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers, iNOW/Chalkable Data Manager and FTE After School Care workers. School directories with parental permission being first obtained. Rapid notification system directory.	No
Home Address	Class I, II, III, depending on use	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers, iNOW/Chalkable Data Manager and FTE After School Care workers	No
Ethnicity*	Class II	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, Assigned Teachers, iNOW/Chalkable Data Manager and FTE After School Care workers	No

National School Lunch Program Status*	Class III	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, CNP Coordinator and staff, iNOW/Chalkable Data Manager, (Point of Sale transactions will be done in such a way as to not identify students who receive free or reduced lunches. Cafeteria managers and CNP employees who process F/R applications or lists of benefit recipients will ensure the information is secure and made available only to those persons who require it.)	No
ESL Status*	Class II	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, ESL Supervisor, ESL Dept. employees, Assigned Teachers, iNOW/Chalkable Data Manager, ESL School Committee members and FTE After School Care workers	No
Special Ed Status*	Class III	Principal, Asst. Principal, Counselor, Registrar, Testing Coordinator, Special Ed Coordinator, Special Ed. Case Worker, iNOW/Chalkable Data Manager, Bus Drivers, and Assigned Teachers	No
Medical Conditions	Class III, except in emergencies	Principal, Asst. Principal, Registrar, Nurse, Immediate Teacher, Lunch Room personnel (if food allergy), iNOW/Chalkable Data Manager, Bus Drivers, Special Education Personnel and FTE After School Care workers, if applicable	No
Grades	Class III, except when used in conjunction with honor rolls/awards	Principal, Asst. Principal, Registrar Immediate Teachers, Student, Parents or legal guardian, School Counselor, Gifted Teacher (only for students assigned), PST Committees, Appropriate Central Office Administrators, Testing Coordinator, iNOW/Chalkable Data Manager, Transfer to schools and Scholarship applications, C2C	INOW Parent Portal - Access is to be given to parents or legal guardians only. INOW Teacher web access

Attendance*	Class III	Principal, Asst. Principal, Attendance Clerk, Registrar, Student Services Coordinator and staff, Truancy Officers, School Resource Officer, Immediate Teachers, PST Committee iNOW/Chalkable Data Manager. Parent Involvement Specialist	INOW Parent Portal only
Discipline*	Class III	Principal, Asst. Principal, Counselor, SRO,	No
		Registrar, Student Services, iNOW/Chalkable Data Manager, Intervention Team Members, Immediate Teachers, Special Plans Members	
Standardized Test Scores*	Class III	Principal, Asst. Principal, Registrar, Immediate Teachers, Testing Coordinator, Appropriate Central Office Personnel, PST Committee, iNOW/Chalkable Data Manager, Counselors, EL Cooridinator, EL Teacher, Instructional Coach, Special Education Personnel, Student, Parent	No
System Benchmark Test Scores	Class III	Principal, Asst. Principal, Registrar, Immediate Teachers, Testing Coordinator, Appropriate Central Office Personnel, PST Committee, iNOW/Chalkable Data Manager, Counselors, EL Cooridinator, EL Teacher, Instructional Coach, Special Education Personnel, Student, Parent	No
*ALSDE may access all such information for State Reporting Collection purposes			

*ALSDE may access all such information for State Reporting Collection purposes

Data Classifications for Employees

Student Data	Classification	Authorized Users	Web Exposure
Employee Name*	Class I or II, depending on use	Human Resources, Principal, INOW/Chalkable Data Manager	Yes

District Employee Number	Class II	Principal, Payroll, Human Resources, and Maintenance staff, as needed	No
Social Security Number*	Class III	Human Resources, Payroll Staff, Principal, INOW/Chalkable Data Manager	No
Home Phone Number	Class II	Human Resources, Principal, Payroll Staff, INOW/Chalkable Data Manager, school directories with employee permission, Rapid notification system directory	No
Home Address	Class III	Human Resources, Principal, INOW/Chalkable Data Manager, Payroll Staff	No
Ethnicity*	Class II	Human Resources, Principal, Payroll Staff	No
Medical Conditions	Class III	Human Resources, Principal	No
Certifications*	Class II	Human Resources, Principal Staff, Payroll	No
Attendance	Class III	Human Resources, Payroll Staff, Principal	No
Evaluations*	Class III	Human Resources, Principal	No
College or school transcripts or grades	Class III	Human Resources, Principal	No
HQT Status*	Class II	Human Resources, Principal, Asst. Principal, Registrar, Appropriate Central Office Administrators	Only as needed to comply with any Federal Programs reporting requirements
Prof. Dev. Records*	Class II	Human Resources, Principal, Asst. Principal, Registrar, PD Supervisor, Appropriate Central Office Administrators	No

Benefits	Class III	Human Resources and Payroll Staff	No
Salaries*	Class II	Human Resources, Principal, Asst. Principal, Registrar, Appropriate Central Office Administrators, Payroll Staff	Schedules, but not individual salaries
*ALSDE may access all such information for State Reporting Collection purposes			

II. Compliance

(A) Data Users are expected to respect the confidentiality and privacy of individuals whose records they access; to observe any restrictions that apply to Class III (Sensitive) 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 expressly 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 personal curiosity or that of others.

(B) Each employee at the System will be responsible for being familiar with the System's Data Security Policy and these Security Measures as they relate to his or her position and job duties. It is the express responsibility of Authorized Users and their respective supervisors to

safeguard the data they are entrusted with, ensuring compliance with all aspects of this policy and related procedures.

(C) Employees, whether or not they are Authorized Users, are expressly prohibited from installing any program or granting any access within any program to Class III without notifying the Technology Department.

(D) Violations of these Data Security Measures may result in loss of data access privileges, administrative actions, personnel actions, reprimand and/or personal civil and/or criminal liability.

III. Implementation of Network/Workstation Controls and Protections and Physical Security

(A) Authorized Users

1) Authorized Users are responsible for being knowledgeable in all policies, laws, rules, and best practices relative to the data for which they are granted access; including, but not limited to FERPA, HIPAA, etc.

2) Authorized Users shall be responsible for informing appropriate Technology Department personnel about data classifications in order that the Technology Department can determine the best physical and/or logical controls available to protect the data. This shall include:

a. Which data should be classified as Class III
b. Where that data resides (which software program(s) and servers)
c. Who should have access to that data (Authorized Users)
d. What level of control the Authorized User should have to that data (i.e. read only, read/write, print, etc.)

(B) Location of Data and Physical Security

1) Class III data shall be stored on servers/computers, which are subject to network/workstation controls and permissions. It shall not be stored on portable media that cannot be subjected to password, encryption, or other protections.

2) Serving devices (servers) storing sensitive information shall be operated by professional network system administrators, in compliance with all Technology Department security and administration standards and policies, and shall remain under the oversight of Technology Department supervisors.

3) Persons who must take data out of the protected network environment (transport data on a laptop, etc.) must have the permission of their supervisor prior to doing so. Permission to do so will be granted only when absolutely necessary, and the person transporting the data will be responsible for the security of that data, including theft or accidental loss.

4) All servers containing system data will be located in secured areas with limited access. At the school or other local building level, the principal or other location supervisor will ensure limited, appropriate access to these physically secured areas.

5) District staff who must print reports that contain Class II or III data shall take responsibility for keeping this material in a secure location – vault, locked file cabinet, etc. In addition, all printed material containing Class III documentation shall be shredded when no longer in use.

(C) Disposal of Hardware containing System Data

1) Prior to disposal of any computer, the user will notify the Technology Department. A technician will remove the hard drive from the device and destroy it prior to the device being disposed of or auctioned off.

2) All schools and departments which purchase or lease copy machines or multifunction printers will be expected to include provisions for the destruction of data on the device's hard drive or the destruction of the hard drive itself prior to disposing of the copier or MFP or its return the leasing agency. (See Exhibit C.)

(D) Application of Network and Computer Access Permissions

1) The Technology Department staff shall be responsible for implementing network protection measures that prevent unauthorized intrusions, damage, and access to all storage and transport mediums; including, but not limited to:

a. Maintaining firewall protection access to the network and/or workstations.

b. Protecting the network from unauthorized access through wireless devices or tapping of wired media, including establishing 'guest' wireless networks with limited network permissions.

c. Implementing virus and malware security measures throughout the network and on all portable computers.

d. Applying all appropriate security patches.

e. All servers and devices housing sensitive data shall be maintained at a version actively supported by the device's software and hardware manufacturers to ensure availability of applicable security patches.

f. Establishing and maintaining password policies and controls on access to the network, workstations, and other data depositories.

2) Technology Department staff will apply protection measures based on the Data Classifications (see sections IV and V), including:

a. Categorizing and/or re-classifying data elements and views.

b. Granting selective access to System Data.

c. Documenting any deviation from mandatory requirements and implementing adequate compensating control(s).

d. Conducting periodic access control assessments of any sensitive information devices or services.

(E) Sensitive Data as it pertains to Desktops/Laptops/Workstations/Mobile Devices

1) Firewalls and anti-virus software must be installed on all desktops, laptops and workstations that access or store sensitive information, and a procedure must be implemented to ensure that critical operating system security patches are applied in a timely manner.

2) Storage of sensitive information on laptops, mobile devices, and devices that are not used or configured to operate as servers is prohibited, unless such information is encrypted in a Technology Department-approved encryption format.

3) The user responsible for the device shall take proper care to isolate and protect files containing sensitive information from inadvertent or unauthorized access.

4) Assistance with securing sensitive information may be obtained from school-level Technology Coordinators with input from the Technology Department, as necessary.

IV. Transfer of Data to External Service Provider

(A) Student Class I data, directory information, and, in some cases Class II data, may be transferred to an external service provider, such as an online website that teachers wish students to use for educational purposes. Provide that:

1) The teacher follows the protocols for getting approval for the site to be used.
2) The District notifies parents about their right to restrict their child's data from being shared with such sites annually.
3) The transfer of data is handled in a manner approved by the Technology Department, or is performed by the Technology Department.

(B) No Class III data, or FERPA protected educational records, will be transferred to an external service provider without prior approval of the Data Governance committee. Exception: Alabama State Department of Education.

(C) No school or department should enter into a contract for the use of any program that requires the import of District data without first consulting and receiving approval from the Data Governance committee.

(D) The Data Governance committee will determine which of the following should be required of the service provider and assist in ensuring these requirements are met prior to any data transfer:

1) Contract
2) Designating the service provider as an "Official" as defined in FERPA
3) Memorandum of Understanding
4) Memorandum of Agreement
5) Non-Disclosure Agreement

(E) Non-Disclosure Agreement (NDA) Information

A. When to Use a Non-Disclosure Agreement

1. Private Information. Confidential information, as defined by FERPA and other regulations and policies, is to be protected and disclosed only to those employees who have a direct legitimate reason for access to the data in order to provide educational services to the student.

2. You must seek guidance from the Student Services, Special Education, and/or the Technology Department prior to transferring confidential information to any outside company, online service (free websites), or to any outside individual, organization, or agency without the explicit written permission of the parent of a minor student or an adult-aged student. This information includes:

1) Social Security number
2) Grades and test scores (local and standardized)
3) Special education information
4) Health information and 504 information
5) Attendance information (not enrollment, but specific attendance dates)
6) Family/homeless/or other similar status
7) Child Nutrition Program status (free or reduced meals)

This includes providing confidential information to individuals, including System employees, for use in dissertations or other studies for college courses or doctorial studies. Refer all such requests, including those for federal, state, or other studies to the Instruction Department and the Technology Department for their approval before releasing any such individualized information. Approved recipients may be required to complete an NDA so that they fully
understand their responsibilities with regard to safeguarding and later destroying this private information. This restriction does not apply to publicly available aggregated data such as dropout rates, attendance rates, percentage of free and reduced lunch program students.

Exceptions. Other Public K-12 Schools - Private information may be transferred upon request to the State Department of Education or other public school systems with a

legitimate need for the data; however, the transfer process should comply with data security protocols (see below). In addition, personnel must research all recipients to ensure that the school is legitimately a public school rather than a private school.

Colleges – Confidential information may be transferred to institutions of higher education, when the adult student or the parent of a minor student requests that transcripts or other private information be released to specific institutions. Such information should not be transferred to colleges based on a request from the college directly, unless approved by the individual whose records will be transferred.

3. Directory Information. Although Dothan City Schools has identified the following as "Directory Information," schools should still carefully consider the transfer or publication of this information. Seek guidance when in doubt. Much of this information, combined with data collected elsewhere can be used for identity theft purposes, stalking, and other unlawful or unethical purposes.

1) Home address
2) Home or cell phone numbers of students or their parents
3) Email addresses of students or their parents
4) Date and place of birth

Exception: U.S. Military and institutions of higher learning for recruiting purposes. However, school must first determine which parents have submitted Opt Out forms relative to these requests prior to transferring data.

(E) Non-Disclosure Agreement Processing

1) The Technology Department will keep all NDAs on file. This will eliminate the need for each school to solicit an NDA from companies, which already have NDAs on file. Technology will also ensure that the NDA is renewed annually where necessary.
2) What the school should do:
a. Get the following specific information from the "entity" to which you want to transfer the information: company name, web address, phone number, fax number, and email address, name of individual you are working with.
b. List the information you wish to transfer to the 'entity'
c. Send this information to the Technology Department for referral to the Data Governance Committee.
3) Upon approval by the Data Governance Committee, the Technology Department will determine if there is a current NDA already on file with the entity. If not, one will be prepared and sent to them. Once the agreement has been signed, the Technology Department will notify the school and oversee the process of securing uploading the necessary data to the service provider.

4) Note that all confidential data that will be transferred by email, whether in the body of the email or as an attached file, should be encrypted. The Technology Department can help you with transporting this data.

(F) Sample Non-Disclosure Agreement

1. Refer to Exhibit D for a copy of the NDA (Non-Disclosure Agreement)

V. Reporting Security Breaches
All employees shall be responsible for reporting suspected or actual breaches of data security whether due to inappropriate actions, carelessness, loss/theft of devices, or failures of technical security measures.

Data Governance Training
I. School Staff
(A) School Staff including Central Office Administrators, Registrars, Counselors, and Teachers will review refresher training on FERPA and other data security procedures posted annually on the Dothan City Schools Web Site and electronically sign completion.
(B) All department heads will be expected to educate their support staff on data governance as it applies to their department's work.
(C) All users will receive reminders throughout the year via email regarding malware threats and phishing scams and how to report suspected threats.
(D) School administrators shall educate PTOs, boosters, and other parent groups about FERPA and student confidentiality. For instance, organizations that intend to post information about the school's students or activities should not compromise the privacy of students in protective custody. Because the school cannot tell these groups which students may be in such situations, the organization should be cautioned about exposing any information or photos that could cause harm to students or their families.
(E) The Technology Department shall have procedures that include educational materials for booster organizations that wish to post their own websites. This shall include both FERPA and COPPA information.

Data Quality Controls
I. Job Descriptions
(A) 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: school registrars, counselors, special education staff, and CNP staff handling free and reduced lunch data.
(B) Teachers shall have the responsibility to enter grades accurately and in a timely manner.
(C) School administrators shall have the responsibility to enter discipline information accurately and in a timely manner.

II. Supervisory Responsibilities

(A) It is the responsibility of all Supervisors to set expectations for data quality and to evaluate their staff's performance relative to these expectations annually.

(B) 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.

Student Information Systems

I. Student Information Applications

(A) Any software system owned or managed by the District, which is used to store, process, or analyze student 'educational records' as defined by FERPA shall be subject to strict security measures. These systems are:

1) INOW – General student information system
2) SetsWeb – Special Education information system
3) Franklin/Newton – Child nutrition information system

(B) Administrators with supervisory responsibilities over the District's Student Information Systems shall determine the appropriate access rights to the data and enforce compliance with these roles and permissions.

II. INOW Access

INOW enables authorized users to access the application from anywhere they may have Internet access. In response to this anywhere/anytime access, as well as the fact that INOW provides less-granular permission settings than its predecessor, the Data Governance Committee and its, INOW permissions sub-committee, has implemented the following:

(A) Strong password requirement for INOW logins

(B) Data Security Agreements for those with INOW permissions who are not teachers (Refer to Exhibit E.) should be read and signed electronically for all applicable personnel.

(C) 'Notification of Risks' to school administrators and registrars

1. INOW Access for Parent Volunteers

Some schools rely on parent volunteers to help greet visitors and locate students. Due to FERPA and other confidentiality expectations volunteers should only be granted very limited INOW rights. In most cases this should be the 'Schedule Lookup' level of access which enables the volunteer to see a list of all students and their schedules.

Remember, INOW permissions are web-based so what volunteers can see from the school, they can also access from anywhere they have Internet access.

2. Concerns about Parent Volunteers Checking Students Out of School

Releasing a child from school into the care of someone else is a serious responsibility. Schools should carefully assess whether or not the information in INOW for this purpose is always up to date. In the past registrars have raised concerns that parents often change their minds about who can and cannot check out their children, but they

don't necessarily notify the school in a timely manner. This makes the prospect of allowing parent volunteers who are unfamiliar with the current circumstances of various family situations to check out students an area of concern. Student Services will be providing recommendations regarding this important function.

3. Allowing Others to Use Another User's INOW Account to 'Give' them Greater Access is Prohibited

A user's INOW permission level is based on their job responsibilities. Violating FERPA can have serious consequences, including the loss of Federal Funding and other legal liabilities. Since we have a

responsibility to protect our student and employee data from identity theft or other misuse, no one may log into INOW and allow others to use their access. Participating in this practice violates our Acceptable Use policies and Data Security Procedures.

The Technology Department will perform random scans to determine if the same INOW user id is in use concurrently on two separate computers and investigate these occurrences as warranted. Registrars who are using multiple machines have been instructed to notify Technology of this so that dual logins on specific IP addresses will not be viewed as a potential violation of this rule.

4. Plan for when your Registrar is Out for an Extended Period

You should have a plan for occasions when your registrar is out sick or on vacation. Anyone filling in for the registrar should be a bona fide employee, not a volunteer. Technology will attempt to help in extreme situations, but our ability to do so is limited.

5. Providing Information to Others on Students NOT Enrolled at Your School

INOW rights intentionally prevent the staff at one school from seeing information on students at another school, which complies with FERPA guidelines. The only exception is for district level personnel who have specific needs to see all school data and teachers or others who serve specific students in multiple schools.

It is important that staff members at one school do not attempt to give information about students enrolled in another school to individuals who ask for such information. Instead they should expect the person asking for the information to contact that school himself or herself. If the person asking for information does not know what school to contact, then they should be referred to the Curriculum Department.

DO NOT tell an individual who has no official right to know where else the student is enrolled. Even if the person asking is a parent, there may be a dangerous situation that you are unaware of, so the safe action to take is to refer such requests to the Curriculum Department.

The danger in telling someone, employee or not, what other school the child is enrolled in lies in the fact that you have no access to that student's record and will not know if the child is in protective custody or is involved in some other situation such as custody dispute, etc. This could result in a safety issue.

This rule applies even when the person asking for the information is one of our own employees. Unless the person requesting the information is currently providing

educational services to that student, they should not be given any information about them, including where the student is enrolled. And, if they are providing educational services to a student at another school, but claim not to know where the child is enrolled, then this should raise some flags. In this case, contact Student Services for guidance.

INOW Permission Standards for Dothan City Schools

I. Permission Committee

(A) INOW Permissions committee members include:

1) Technology Coordinator/Data Governance Committee chairperson
2) INOW central support staff and network administrator responsible for INOW
3) Students Service department representatives
4) Principal representatives
5) Testing/Counseling representative

(B) Requests for changes to the standards, set by the INOW Permissions committee can be made at any time by a school or District-level administrator. School administrators will be notified prior to the annual committee meeting so that they can submit requests in writing prior to that date for consideration.

(C) Changes to settings may also be made by the committee decision as a result of software changes, new job roles, other local factors, and directives from the State, or as determined by the Superintendent.

(D) The permissions are granted to individuals officially serving in the roles shown below. However, these permissions will not be granted automatically. The individual's principal/supervisor must endorse them by submitting their name to the Technology Department. Principals and supervisors will be asked to renew their endorsements annually. In addition, these endorsements may be revoked if the principal, supervisor, or the committee determines that the access is no longer necessary or has other reasonable concerns. The INOW Permissions Committee makes the final determination for access settings.
(E) The INOW Permissions committee will meet annually in order to review permissions and to consider new requests. Requests that are made between annual meetings will be presented to the members via email or in-person, as appropriate. Changes will be conveyed to affected personnel via memos and updates to the manual and web site. (See Exhibit A.)

II. Allowable INOW Permission Settings

Group: Find Student Only (Schedule Lookup)
Staff Affected: All INOW Users. (Parent Volunteers may be granted this permission, but only when the INOW Permissions Committee approves a request submitted by a principal.)

All INOW users can use the Look Up feature to find any student's current location. The staff can also refer to a Student Schedule Matrix pdf file which the school's Registrar will post to the Faculty Share. Registrars will update the file as needed.

Only Technology INOW administrators can add individuals to this permission group.

Group: Check In/Out
Staff Affected: Assigned by Technology upon request
This level of permission allows the user to see the Summary, Main, and Contacts tabs.
It gives them the ability to check students in and out and to view the following information:

- Name
- Date of Birth
- Age
- Phone (This can be hidden if necessary)
- Gender
- Grade (This can be hidden if necessary)
- Address (This can be hidden if necessary)
- List of Contacts and their relationship and phone numbers

The user will see the special symbols, but not open up these notes to see what instructions they contain.
Only Technology INOW administrators can add individuals to this permission group.

Group: Limited Student View Staff Affected: Library Media Specialists*
Staff with "Limited Student View" permissions will have Read-Only rights to contact information for all students in the school.
*Library Media Specialist may have additional permissions if they give grades or serve in other roles within the school.
Only Technology INOW administrators can add individuals to this permission group.

Group: Test Data Entry

Staff Affected: Secretaries in counseling offices (if requested by principal) These permissions enable staff to enter testing data.
Only Technology INOW administrators can add individuals to this permission group.

Group: Special Student View

Staff Affected: Individuals serving in the following roles, when endorsed by the principal/supervisor
- Athletic Directors (Can also be added to AD Quick Entry Edit Group, see below)
- Lead Special Ed Teachers
- Lead ESL Teachers
- PST Chairperson

Staff with "Special Student View" permissions will be able to see the following information for ALL students in the school:
- Contacts – full records
- Grades which have been posted by teacher
- Attendance profile
- Schedules

Principals may also want to ask Registrars to set up Non-Reporting Class Rosters (see below) for individuals who have been granted Special Student View permissions. Or, they may want to request that these individuals be set up with Non-Reporting Class Rosters instead of being given the Special Student View. In either case, Non-Reporting Classes can make it easier for individuals to look up information on the students they are responsible for because it will enable them to check each student's information from a 'class' roster (i.e. football, PST, girl athletes, etc.) rather than look up each student by name in INOW. Creating these 'Non-Reporting Class Rosters' will take more work on the Registrar's part. However, it is a good option when principals want to restrict access to only the students served by the individual, rather than all students in the school.

Group: Athletic Directors Quick Entry & Future Year Staff Affected: Athletic Directors only
Middle and high school athletic directors will be given the ability to use the Quick Entry Edit feature in INOW to edit students' eligibility settings, but only after being trained by the school registrar.
Athletic Directors with this permission must sign the associated Security Agreement.

Group: Non-Reporting Class Rosters Staff Affected: Various
When teachers have a formal responsibility to support students who they do not have on a class roll, and this responsibility includes viewing the students' grades, then the Registrar may be asked to set up a Non-Reporting Class for that teacher. Examples of these situations/individuals include:

- Special Education teachers with students on their caseload, but who are not in their class
- Academics First Sponsor
- Math or Reading Coaches, where applicable
- Gifted advisors, where applicable
- Anyone who already has or would be eligible for the Special Student View (above)

Once the 'class' is created, the 'teacher' will have the ability to 'print' a comprehensive progress report for the students which will give the 'teacher' access to posted grades from all classes.
Keep in mind that this will take some work on the Registrar's part. In the case of the Athletic Director and a separate Academics First teacher, they could both be listed as teachers for the non-reporting class to minimize the work involved.
The Technology Department will provide Registrars with directions for creating these non- reporting classes. These directions must be followed carefully so that the courses do not affect attendance, LEAPS,

or other state reports. These courses will need to be scheduled outside of the school day, must be tagged as a non-reporting course in the Master Schedule, and must use the correct State Course Number.

Group: Discipline History Staff Affected: Administrators Only
Only school administrators will have access to student discipline history. Staff should consult with their school administrators if they need discipline history on a given student.
AHSAA Student in Good Standing Forms –
The AHSAA Student in Good Standing Release Form must be completed and signed by the school Principal. This is only to be completed when the student athletes leaving your school are not in good standing.

III. INOW Substitute Teacher Set Up & Roles

All Subs and Temporary Employees who are granted INOW access must sign the STI Security Agreement. The school registrar should facilitate this and store the Agreement at the school. If a Long Term Sub works at more than one school, each school should have a signed Agreement on file.
When possible, the teacher going on leave should set up the class grade book before the Long Term Sub takes over. Technology INOW administrators can assist in setting up grade books if the teacher is not able to do so prior to his/her absence.

Group: Substitute Teacher Access
Staff Affected: Long Term Subs and Temporary Employees

Scenario 1: Short Term Sub (under 21 days)

INOW: No access

- If the teacher does not return after 20 days, then the sub may have INOW access as a Long Term Sub. Select the appropriate Scenario from those listed below.

- If it is known in advance that the teacher will be out for longer than 20 days but less than 1 semester then use either Scenario 2 or 3, whichever applies.

Scenario 2: Sub over 21 days, but less than 1 Semester (aka Long Term Sub)

INOW Role: Long Term Sub INOW Schedule: Additional Teacher

Scenario 3: Long Term Sub/Temporary Employee* for more than 1 semester, but less than 1 year

INOW Role: Long Term Sub INOW Schedule: Additional Teacher

EXCEPTION: If the original teacher will not be returning to your school (i.e. transferring, resigning, retiring, etc.) then they should be removed from the master schedule and the teacher replacing them should be shown as:

INOW Role: Long Term Sub
INOW Schedule: Teacher

Scenario 4: Temporary Employee* for one full year

If the original teacher has highest degree and years of experience, then the Temporary Employee will have:

INOW Role for Temporary Employee: Long Term Sub INOW Schedule for Temporary Employee: Additional Teacher INOW Role for Teacher on Leave: First Primary Teacher INOW Schedule for Teacher on Leave: Teacher

If the temporary employee has highest degree and years of experience, then the Temporary Employee will have:

INOW Role: First Primary Teacher
INOW Schedule: Teacher INOW Role for Teacher on Leave: None INOW Schedule for Teacher on Leave: None

Email Use and Security Agreement

I. User Agreement

All individuals issued an email account by Dothan City Schools are expected to follow the District's Email Use and Security Agreement. This agreement is provided all new staff. (See Exhibit B.)

II. Dothan City Schools Email Disclaimer

This message, and any files transmitted with it, may contain confidential information and is intended only for the individual addressee(s). If you are not the named addressee or if you have received this email by mistake, you should not disseminate, print, distribute or copy this e-mail. If you have received this email by mistake, please notify the sender immediately and delete this e-mail from your system. Employees of Dothan City Board of Education are expressly required not to make defamatory statements and not to infringe or authorize any infringement of copyright or any other legal right by email communications. Any such communication is contrary to Board policy and outside the scope of the employment of the individual concerned.

Banking Security

I. ACH Transfers

The CFO should notify the Technology Coordinator of any plans to change its electronic banking processes. The Technology Department will assist in evaluating whether or not any such practices would pose an unacceptable risk to the District's network.

II. Bank Balance Auditing Recommendations for Preventing Electronic Theft

The Technology Department highly recommends that the District and school bank balances which employ electronic payment measures, be checked daily, or within the timeframe given by the bank, in order to report fraudulent withdrawals in order to recover stolen funds.

Data Backup and Retention Procedures

The following standards may be updated, amended, or changed as needed. Any changes will be clearly marked and prior versions will be kept available for review.

I. Scope

(A) This procedure applies to all servers and systems installed and controlled exclusively by the Dothan City Schools Technology Department and excludes servers and systems controlled by specific departments within Dothan City Schools. In cases where other Departments are responsible for their backup systems, the Technology Department will provide technical and professional guidance for backup routines and procedures, as requested.

(B) This procedure applies to all user data in the following manner:

All users with network permissions are trained and urged to store data onto their server workspace, but they are permitted to store files on local machines. Individual users may delete their data from either

network servers or local machines at will. If data stored on a server is deleted by the end user and falls outside of the backup period the System has no method of recovering such files.

Files stored by users on individual hard drives or other individual storage devices are not backed up and may become unrecoverable in the case of hard drive failure or accidental deletion..
Although technicians may be able to locate or recover locally stored files, these files are not part of the data backup or recovery plan.

(C) This procedure does not apply to connected systems that are the property, and therefore the responsibility, of outside entities such as the Alabama State Department of Education.

II. General System Data Backup Procedures

(A) Source Server Data Shadow Copy

1) As data is changed, replaced or deleted on school and district servers, older versions of that data are preserved.

2) Data Shadow Copy occurs automatically once per day, Monday thru Friday.

3) Includes any data that has been added or modified in the last 24 hours.

4) Data Shadow Copy versions are housed on the same servers which originally contained the data.

5) Servers are physically isolated from students and most faculty members to protect from tampering and disturbance.

(B) Incremental Backups

1) System Data that has been added or modified since the last backup operation is backed up to centralized devices.

2) Incremental Backups occur automatically once per day, 7 days a week.

3) Data Backup devices are housed outside of the Network Operation Center (NOC) for increased security and protection.

III. E-mail Data Backup Procedures

(A) Dothan City Schools email is stored within the cloud by Google and backed-up by Google Vault.

IV. Time Frames for Data Retention
(A) All statements of data retention, and the subsequent ability to restore that retained data, are subject to hardware and software components functioning properly.

(B) The time frames listed below are based on what time frames are currently possible and affordable with current staff and funds for backup servers and media. Time frames may change depending on the amount of data the System generates and the budget provided to manage these services.

(C) Data Retention timeframe is expressed as a minimal amount of time for which any protected data should be recoverable, utilizing the multiple protection mechanisms available under normal circumstances.

(D) In the event of a catastrophic event, such as the destruction of the Network Operations Center, some levels of data recovery will be affected, but recovery will still be possible to some point within the last 7 days provided off-site locations have not been similarly destroyed.

(E) Retention of General System Data.

1) Retained for normal restores for a period of one week.
2) Stored off-site.

(F) E-Mail Data is maintained in the cloud by Google, backed up by Google Vault and not backed-up by Dothan City Schools.

(G) Retention of Web Traffic and Browsing Data.

1) There is currently no system in place to retain Web Traffic and Web Browsing Data. Older data is cleared from system within hours of its recording, due to the high rate of new incoming data.

(H) Backup logs will be maintained by automatically.

(I) Litigation Holds

1) It shall be the responsibility of the Central Office administrators to promptly inform the Technology Department of any pending litigation where user files or emails may become part of eDiscovery requests.
2) Once notified, the Technology Department will take all available actions to retain all affected files and emails, such that they are not deleted according to the retention schedules above.

V. INOW Alabama State Back Up

(A) Student Information System - Offsite Remote Backup
1) Currently an offsite backup provided by Software Technology Incorporated (STI) in conjunction with Enveloc Inc. is in place. From the Student Information Systems source database, a nightly scheduled process occurs to compress, encrypt, and transmit one copy of the InformationNow database backup to the Enveloc storage cloud. This file is accessible for remote access provided that the user account, encryption key, and password are all provided and active.

2) Access to prior years student data may be limited/unavailable due to the changeover from the STI Legacy program to the new web based INOW program. Structural changes to the table design in some cases may prevent access to certain areas of the data as well as the discontinuation of support for the Legacy program.

VI. Email Archiving

(A) Dothan City Schools does not archive email and depends on Google Vault for backup. The current policy covered by the AUP is to retain hard copies of any emails that could potentially lead to litigation.

(B) Google Apps for Education was implemented for students in grades 4-12
and for staff. Email, using the domain address @dthnstudent.net, will be part of this implementation. This is an auxiliary email account and is intended to be used between students and teachers for instructional use only. Google hosts this email system. It will not be backed-up by the District. The District's Google Apps administrators can download mailbox contents on an as-needed basis to recover deleted items or conduct investigations. The search capabilities of this system are limited and the length of time these mailboxes are

kept available is not within our control. In addition, if the District exits the Google Apps for Education program, this data will become unavailable to the District.

VII. Data Included / Excluded

(A) Data which should be included in the Data Backup System:

1) iNOW
2) CNP Data
3) Faculty home directories
4) Faculty shared data areas
5) Student home directories
6) Student shared data areas
7) Backups repository on all servers, encompassing:
7.1) SQL database backups
7.2) SQL applications (such as ACT)
7.3) Server System State

(E) Excluded data is generally excluded because it is especially large AND appears in the same format and version on multiple servers throughout the school system.

1) Data specifically Excluded from the DataBackup System:

a) Server Operating System, swap files, temp files & lock files.
b) Ghost files and ISO image files.
c) Uncompressed backup or transaction files
d) Static data that is replicated on multiple servers (i.e. Lee Vs. Macon)
e) Any directory that's name begins with an exclamation point (!)
f) STI Legacy Data - final copy of legacy data is stored a separate server.

VIII. Data Restore Procedures

(A) In the event that a network user requires that data be restored from the Data Backup System, they shall do one of the following:

1) Contact the Technology Help Desk
2) Contact their School Technology Coordinator (TC)
3) Contact the District Network Administrator

(B) Restores shall be given High Priority treatment and initiated in an expedited manner.

Restrictions on Parents Posting Images of Students (who are not their own children) to Social Media

With respect to pictures of students being posted online on sites that are not on our servers, we are trying to prohibit this for our staff and discouraging it for parents. We try to support our schools in discouraging parents from posting pictures of other children on the web. Coming to school is different than joining a little league team or some other voluntary activity. We don't think the classroom teacher or the school could give an individual the right to post pictures of his/her class online without having control of the site and ensuring that every other parent has agreed to this and has access. From our department's standpoint, we think all material posted online about school should be on our servers or a server such as Edmodo which we have control over and administrative access to.

Exhibit A: - Examples of INOW Permissions Memoranda

DATE: <Date>
TO: School and District Administrators RE: INOW Permissions
FROM: INOW Permissions Committee

The INow Permissions Committee met on <Date> to review our standards and discuss possible changes. The committee determined that our current standards remain effective in terms of balancing various employees' need for access with our responsibility to keep student and employee information confidential. The following information is important, please read this entire memo.

Summary of New Permissions & Standards

Athletic Directors
Middle and high school athletic directors will be given the ability to use the Quick Entry Edit feature in INOW to edit students' eligibility settings, but only after being trained by the school registrar.

Check In/Check Out Permission Group
A new level of permissions for staff checking students in and out has been established. This permission level has slightly more access than Schedule Lookup, which is typically used by parent volunteers. (See permissions descriptions that follow.) Only Technology INOW administrators can add individuals to this permission group.

Long Term Subs & INOW Permissions
See the INOW Permission Handbook section of this memo for details.
All Subs and Temporary Employees who are granted INOW access must sign the STI Security Agreement. The school registrar should facilitate this and store the Agreement at the school. If a Long Term Sub works at more than one school, each school should have a signed Agreement on file.

When possible, the teacher going on leave should set up the class grade book before the Long Term Sub takes over. Technology INOW administrators can assist in setting up grade books if the teacher is not able to do so prior to his/her absence.

Exhibit B: Email User Agreement
Electronic communications, in its many forms, can be a very efficient and effective method of communicating with others; however, it has many inherent risks. Once sent or posted, the author no longer has control over the information contained in the message or posting. The purpose of this Acknowledgement is to make Dothan City Board of Education employees and others granted network accounts aware of certain risks and responsibilities that accompany using electronic communications provided by Dothan City Schools.
This Acknowledgement provides guidance on the professional, ethical, legal, and responsible use of System electronic communications (E-mail, list serve, web site, etc.). This document does not constitute all rules concerning electronic communications. Refer to Dothan City Schools' web site for a complete list of policies.
This Acknowledgement applies to all full-time employees, part-time employees, contracted employees, temporary employees, and other agents operating on behalf of Dothan City Schools. It applies to any person or group of persons who have E-mail accounts, and also to those who request that an account holder send a message on their behalf. It is applicable to all electronic communications regardless of the physical location (school, office, home, or any other offsite location) of the user.
Prohibited Use
The Dothan City Schools' electronic communications programs shall not be used for the creation or distribution of any content that:
- Discloses unauthorized or restricted information to inside or outside parties via electronic communications, including restricted or confidential information that would violate the privacy of individuals or violate any other local, state, or federal laws including, but not limited to FERPA and HIPAA.

- Contains private information such as student grades, discipline incidents, suspensions, social security numbers, special education status, or Individualized Education Plans in cases where it would violate FERPA.
- Discloses personal information regarding students, faculty, staff, or parents to third parties.
- Contains information that pertains to someone other than the addressee (For instance, do not address E-mails to numerous individuals that contains private information that does not apply to all of the recipients).
- Defames, slanders, or libels another person or organization.
- Contains or links to pornography or other content inappropriate for K-12.
- Contains content that may be considered offensive or discriminatory, including, race, gender, hair color, disabilities, age, sexual orientation, religious beliefs and practice, political beliefs, or national origin.
- Contains content or files that violate any copyright or trademark law. Users should be aware that passing on E-mails that contain copyrighted or trademarked material may make them liable in copyright or trademark infringement cases even though they were not the original sender.
- Intentionally contains malicious or harmful software such as computer viruses and spyware.
- Contains fraudulent, harassing, or intimidating content.
- Violates any license governing use of software.
- Is intended for personal or private financial gain.

In addition, should employees receive electronic communications that contain such information, they should not forward such messages on to others whether inside or outside the System.

Personal Use

Occasional use of the E-mail system for personal use is permitted with certain limitations. Personal E-mails should be kept in a separate folder with the user's Google account and stored for no longer than 1 month. Except in cases of emergency, users should refrain from sending and reviewing personal E-mails during work hours. The content of personal E-mails, whether being received or sent, must also conform to the standards listed above as prohibited, and other restrictions that may be found in the Dothan City Board of Education Employee Acceptable Use Policies. Users should immediately delete inappropriate E-mails and inform the sender about the restrictions on acceptable content.

Dothan City Schools E-mail addresses shall not be used for non-work related shopping, subscriptions, memberships. In addition, Dothan City Schools E-mail addresses should not be used on personal websites, blogs, social networking accounts, online forums, or any other electronic medium.

E-mail Filtering

Dothan City Schools attempts to block offensive messages and spam from entering our System; however, this process is not 100% effective. Employees should report offensive and spam messages by forwarding them to spam@dothan.k12.al.us or by contacting the Technology Department. Such messages should never be intentionally forwarded on to others whether inside or outside the Dothan City Schools E-mail directory.

Mass E-mails

E-mails intended for all employees in the Dothan City System must be approved by the Superintendent, his designee, or the Technology Coordinator prior to be being sent.

Monitoring and Waiver of Privacy

Dothan City Schools is not obligated to monitor E-mail messages; however, authorized administrators of the Dothan City Schools may monitor messages without prior notice. Furthermore, electronic messages and files stored on Dothan City Schools computers or stored elsewhere using a Dothan City Schools E-mail or internet account are deemed to be the property of Dothan City Board of Education. Therefore, Dothan City Board of Education employees and others to which this Acknowledgement applies shall have no expectation of privacy in anything they store, send, or receive on the System's electronic communications systems such as the E-mail system. Employees and others to which this Acknowledgement applies waive any right of privacy they might have in anything they create, store, or receive on the System's computers or electronic communications systems.

Reporting of Violations and Enforcement

Dothan City Schools cannot guarantee that users will not occasionally receive offensive or inappropriate E-mails from outside the System or from fellow employees. Employees may report the matter to an immediate supervisor, the Technology Department, or to System administrators should they feel an incident warrants further investigation.

Any employee found to have willfully misused any form of electronic communications as outlined in this Acknowledgement and in the Employee Handbook may be subject to disciplinary action. These actions may include the suspension or loss of E-mail, web, blog, or other electronic communication privileges; or a verbal or written reprimand. A second violation of an employee may result in an adverse personnel action such as suspension or termination.

Disclaimers
In order to protect the System and the individual, all account holders shall use the disclaimer provided by the System on every E-mail sent. Individuals should be aware, however, that disclaimers do not offer any legal protection in the cases of defamation and libel. In addition, the presence of disclaimers may not entirely protect the sender from civil litigation or criminal prosecution.

Legal Actions
Should any legal actions, civil or criminal, take place which require the production of Dothan City Schools' employees E-mails or electronic files, the System may comply with properly executed legal requests to the extent possible. All legal consequences and associated penalties for civil or criminal violations, shall be the sole responsibility of the account holder and not that of the Dothan City Schools, unless otherwise found by a court of law.
Indemnification
Employees and others to which the Acknowledgement applies agree to indemnify Dothan City Schools for any losses, costs, or damages, including reasonable attorney fees, incurred by Dothan City Schools relating to, or arising out of, their violation of this Acknowledgement.
Modifications
Dothan City Schools may change the provisions of this Acknowledgement. Posting such modifications on the System's electronic communications system or sending such modifications by e-mail, fax, or U. S. Mail shall constitute proper notice of such modifications. However, no one, including principals or supervisors, may modify this procedure in writing or verbally without the consent of the Superintendent.
Acknowledgement
I acknowledge that I have read and understand these risks and conditions, and in consideration of my use of the Dothan City Board of Education computers and/or electronic communications systems. I agree to comply with the terms stated herein. I understand that I can seek further training or explanation regarding the content of this document by contacting my Principal, Supervisor, or the Technology Department.

Printed Name Signature

Date

Exhibit C: Copier Machine Security Recommendations

Many modern copy machines and multifunction printers record images of all information being copied, faxed, or scanned onto their hard drives. In the case of many multifunction machines, an image of every print job, fax, and copy ever made on the machine is retained on its hard drive. In our environment, these images could include FERPA- protected educational records, Social Security numbers, I.E.P.s, and other confidential information. Schools need to be aware that there have been instances where criminals have data-mined copy machine hard drives either disposed of in landfills or taken from previously leased machines.
School administrators should take measures to ensure that the hard drives on any copier or multifunction machine their school uses is properly erased or disposed of when the use of the machine is terminated.
Leases –

Ask the vendor what data protection options are available prior to signing a contract. Add an appropriate option to the contract and be sure to require a Letter of Certification once the machine is returned to the dealer.
Purchases -
Find out if the machine is equipped with data security technology already embedded into it and what this entails.
Enter a ticket for the Technology Department to remove and dispose of the copy machine hard drive prior to sending it to the local landfill or putting it out for auction.

Exhibit D: NDA (Non-Disclosure Agreement)

Nondisclosure Agreement

THIS NONDISCLOSURE AGREEMENT (this "Agreement"), by and between DOTHAN CITY SCHOOLS, AL (the "District"), and (the "Service Provider"), relates to the disclosure of valuable confidential information. The "District" refers to all schools, departments, and other entities within Dothan City Schools. The Service Provider refers to any free or fee-based company, organization, agency, or individual which is providing services to the District or is conducting District-approved academic research. The Disclosing Party and the Receiving Party are sometimes referred to herein, individually as a "Party" and collectively, as the "Parties."

To further the goals of this Agreement, the Parties may disclose to each other, information that the Disclosing Party considers proprietary or confidential.
The disclosure of District's Confidential Information by a Receiving Party may result in loss or damage to the District, its students, parents, employees, or other persons or operations.
Accordingly, the Parties agree as follows:
Confidential Information disclosed under this Agreement by the District shall only be transmitted in compliance with the District's approved security protocols. The Receiving Party must accept the data transmitted in these formats.
The Service Provider will request or receive Confidential Information from the District solely for the purpose of entering into or fulfilling its contractual obligations or pre- approved academic research.
The Service Provider agrees not to use, or assist anyone else to use, any portion or aspect of such Confidential Information for any other purpose, without the District's prior written consent.
The Service Provider will carefully safeguard the District's Confidential Information and may be required to describe such safety measures to the District upon request.

The Service Provider will not disclose any aspect or portion of such Confidential Information to any third party, without the District's prior written consent.

Confidential Information disclosed under this Agreement shall not be installed, accessed or used on any computer, network, server or other electronic medium that is not the property of the District or the Service Provider, or to which third-parties have access, unless otherwise provided in a separate contract or agreement between the Parties hereto.

The Service Provider shall inform the District promptly if the Service Provider discovers that an employee, consultant, representative or other party, or any outside party has made, or is making or threatening to make, unauthorized use of Confidential Information.

The Service Provider shall immediately cease all use of any Confidential Information and return all media and documents containing or incorporating any such Confidential Information within five (5) days to the District after receiving written notice to do so, or whenever the contract for services between the District and the Service Provider expires or is terminated. In addition, the Service Provider may be required by the District to destroy any Confidential Information contained on primary or backup media upon written request of the District.

Date Date

DistrictService Provider

Printed Name Printed Name

Signature Signature

Title Title

Phone/Email Phone/Email

Exhibit E: Chalkable (INOW) Data Security Memo and Agreement

Chalkable Data Security Agreement Memo

Date: <Date>
To: Principals
From: Data Governance Committee
RE: Data Security and Data Security Agreement

As you know, our student employee data should be carefully protected. Not only is much of this information subject to FERPA and HIPAA, but it is also data that could be used for identity theft. In order to ensure that all staff members who have access to Chalkable iNOW understand the important responsibilities that come with such access, we have prepared the attached Chalkable Data Security Agreement form.

Please read the document carefully and notice that it warns against removing personal data on students and employees from the workplace. This type of information should not be carried outside of your school on USB drives, disks, or on laptops. If any of these portable devices were to be lost or stolen, it could put the system at great risk.

Please make enough copies of this document for each of your staff that has Chalkable iNOW permissions to sign. Have them sign the form. Make them a copy of the signed form, and then forward the original to the Technology Department. This will include you, your assistant principals, your counselors, the school nurse, and a few others in your school.

If you have questions, please feel free to contact the Technology Department.

Dothan City Schools Data Security Agreement

Electronic data is very portable and can be vulnerable to theft and unintended disclosure. Therefore, having access to personal and private information as part of one's job duties also carries with it important responsibilities to protect the security and privacy of that data.

As an employee who has access to Dothan City Schools' student and employee data, I understand that I have the responsibility to handle, maintain, and disseminate information contained in these records in a secure manner.

I understand that my access to and dissemination of student and/or employee data is subject to local polices, as well as state and federal laws and statutes. This includes, but is not limited to the Federal Educational Rights and Privacy Act (FERPA) and HIPAA.

I understand that transferring personal information to a third party outside of the school system in any electronic format may only be done after approval by an appropriate Coordinator and the Technology Department.

Except when explicitly instructed to do so by school or district administrators, I understand that copies of student and employee data should never be kept on a temporary storage device such as USB drive or CD; and that student and employee data should not be removed from the school premises on a laptop.
I will keep my computer workstation secure by locking or logging off when the machine is unattended. I will not share network or program passwords with others. I will not allow personal data that has been printed into the view or hands of unintended parties. I will not use my software rights to grant others permission to data to which they are not entitled.
Please sign below to indicate you understand and agree to the above statements.

Printed Name Signature

Date Location

Data Security Agreement: Athletic – Quick Entry Edit Provision
Electronic data is very portable and can be vulnerable to theft and unintended disclosure. Therefore, having access to personal and private information as part of one's job duties also carries with it important responsibilities to protect the security and privacy of that data.
As an employee who has access to Dothan City Schools' student and employee data, I understand that I have the responsibility to handle, maintain, and disseminate information contained in these records in a secure manner.
I understand that my access to and dissemination of student and/or employee data is subject to local polices, as well as state and federal laws and statutes. This includes, but is not limited to the Federal Educational Rights and Privacy Act (FERPA) and HIPAA.
I understand that transferring personal information to a third party outside of the school system in any electronic format may only be done after approval by an appropriate Coordinator and the Technology Department.
Except when explicitly instructed to do so by school or district administrators, I understand that copies of student and employee data should never be kept on a temporary storage device such as USB drive or CD; and that student and employee data should not be removed from the school premises on a laptop.
I will keep my computer workstation secure by locking or logging off when the machine is unattended. I will not share network or program passwords with others. I will not allow personal data that has been printed into the view or hands of unintended parties. I will not use my software rights to grant others permission to data to which they are not entitled.
Athletic – Quick Entry Edit Provision

I understand that access to the Quick Entry Edit utility is being added to my permission so that I may rapidly identify student athletes per the directions provided by the AHSAA. I agree not to delegate this responsibility to others. I will be careful in selecting the Athletic field and the correct students so that the school does not incur unintended insurance costs.
Please sign below to indicate you understand and agree to the above statements.

Printed Name/Title Signature

Date Location

Exhibit F:

Dothan City Schools Technological Services and Systems
Memorandum of Agreement (MOA)

THIS MEMORANDUM OF AGREEMENT, executed and effective as of the day of , 20 , by and between , a corporation organized and existing under the laws of (the "Company"), and DOTHAN CITY SCHOOLS (DCS), a public school system organized and existing under the laws of the state of Alabama (the "School Board"), recites and provides as follows.

Recitals

The Company and the School Board are parties to a certain agreement entitled " " hereafter referred to as (the "Agreement"). In connection with the execution and delivery of the Agreement, the parties wish to make this Memorandum of Agreement (also referred to as MOA or Addendum) a part of the original Agreement in order to clarify and/or make certain modifications to the terms and conditions set forth in the original Agreement.

The Company and the School Board agree that the purpose of such terms and conditions is to ensure compliance with the Family Educational Rights and Privacy Act (FERPA) and the overall privacy and security of student Personally Identifiable Information (PII) hereafter referred to as student information and/or data, including but not limited to (a) the identification of the Company as an entity acting for the School Board in its performance of functions that a School Board employee otherwise would perform; and (b) the establishment of procedures for the protection of PII, including procedures regarding security and security breaches.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is acknowledged hereby, the parties agree as follows.

Agreement

The following provisions shall be deemed to be included in the Agreement:

Confidentiality Obligations Applicable to Certain DCS Student Records. The Company hereby agrees that it shall maintain, in strict confidence and trust, all DCS student records containing personally identifiable information (PII) hereafter referred to as "Student Information". Student information will not be shared with any other resource or entity that is outside the intended purpose of the Agreement.

The Company shall cause each officer, director, employee and other representative who shall have access to DCS Student Records during the term of the Agreement (collectively, the "Authorized Representatives") to maintain in strict confidence and trust all DCS Student Information. The Company shall take all reasonable steps to ensure that no DCS Student information is disclosed to any person or entity except those who (a) are Authorized Representatives of the Company performing functions for DCS under the Agreement and have agreed to be bound by the terms of this Agreement; (b) are authorized representatives of DCS, or (c) are entitled to such DCS student information from the Company pursuant to federal and/or Alabama law. The Company shall use DCS student information, and shall take all reasonable steps necessary to ensure that its Authorized Representatives shall use such information, solely for purposes related to and in fulfillment of the performance by the Company of its obligations pursuant to the Agreement.

The Company shall: (a) designate one of its Authorized Representatives to be responsible for ensuring that the Company and its Authorized Representatives maintain the DCS student information as

confidential; (b) train the other Authorized Representatives with regard to their confidentiality responsibilities hereunder and pursuant to federal and Alabama law; (c) maintain at all times a list of Authorized Representatives with access to DCS student information.

Other Security Requirements. The Company shall maintain all technologies, policies, procedures and practices necessary to secure and protect the confidentiality and integrity of DCS student information, including procedures to (a) establish user IDs and passwords as necessary to protect such information; (b) protect all such user passwords from detection and unauthorized use; (c) prevent hostile or unauthorized intrusion that could result in data corruption, or deny service; (d) prevent and detect computer viruses from spreading to disks, attachments to e-mail, downloaded files, and documents generated by word processing and spreadsheet programs; (e) minimize system downtime; (f) notify DCS

of planned system changes that may impact the security of DCS data; (g) return or destroy DCS data that exceed specified retention schedules; (h) notify DCS of any data storage outside the US; (i) in the event of system failure, enable immediate recovery of DCS information to the previous business day. The Company should guarantee that DCS data will not be sold to, accessed by, or moved by third parties. In the event of a security breach, the Company shall (a) immediately take action to close the breach; (b) notify DCS within 24 hours of Company's first knowledge of the breach, the reasons for or cause of the breach, actions taken to close the breach, and identify the DCS student information compromised by the breach; (c) return compromised DCS data for review; (d) provide communications on the breach to be shared with affected parties and cooperate with DCS efforts to communicate to affected parties by providing DCS with prior review of press releases and any communications to be sent to affected parties; (e) take all legally required, reasonable, and customary measures in working with DCS to remediate the breach which may include toll free telephone support with informed customer services staff to address questions by affected parties and/or provide monitoring services if necessary given the nature and scope of the disclosure; (f) cooperate with DCS by providing information, records and witnesses needed to respond to any government investigation into the disclosure of such records or litigation concerning the breach; and (g) provide DCS with notice within 24 hours of notice or service on Company, whichever occurs first, of any lawsuits resulting from, or government investigations of, the Company's handling of DCS data of any kind, failure to follow security requirements and/or failure to safeguard DCS data. The Company’s compliance with the standards of this provision is subject to verification by DCS personnel or its agent at any time during the term of the Agreement. Said information should only be used for the purposes intended and shall not be shared, sold, or moved to other companies or organizations nor should other companies or organization be allowed access to said information.
Disposition of DCS Data Upon Termination of Agreement

Upon expiration of the term of the Agreement, or upon the earlier termination of the Agreement for any reason, the Company agrees that it promptly shall deliver to the School Board, and shall take all reasonable steps necessary to cause each of its Authorized Representatives promptly to deliver to the School Board, all required DCS student data and/or staff data. The Company hereby acknowledges and agrees that, solely for purposes of receiving access to DCS data and of fulfilling its obligations pursuant to this provision and for no other purpose (including without limitation, entitlement to compensation and other employee benefits), the Company and its Authorized Representatives shall be deemed to be school officials of the School Board, and shall maintain DCS data in accordance with all federal state and local laws, rules and regulations regarding the confidentiality of such records. The non-disclosure obligations of the Company and its Authorized Representatives regarding the information contained in DCS data shall survive termination of the Agreement. The Company shall indemnify and hold harmless the School Board from and against any loss, claim, cost (including attorneys' fees) or damage of any nature arising from or in connection with the breach by the Company or any of its officers, directors, employees, agents or representatives of the obligations of the Company or its Authorized Representatives under this provision.

Certain Representations and Warranties. The Company hereby represents and warrants as follows: (a) the Company has full power and authority to execute the Agreement and this MOA and to perform its obligations hereunder and thereunder; (b) the Agreement and this MOA constitute the valid and binding obligations of the Company, enforceable in accordance with their respective terms, except as such enforceability may be limited by bankruptcy or similar laws affecting the rights of creditors and general principles of equity; and (c) the Company’s execution and delivery of the Agreement and this Addendum and compliance with their respective terms will not violate or constitute a default under, or require the consent of any third party to, any agreement or court order to which the Company is a party or by which it may be bound.

Governing Law; Venue. Notwithstanding any provision contained in the Agreement to the contrary, (a) the Agreement shall be governed by and construed in accordance with the laws of the State of Alabama, without reference to conflict of laws principles; and (b) any dispute hereunder which is not otherwise resolved by the parties hereto shall be decided by a court of competent jurisdiction located in the State of Alabama.

IN WITNESS WHEREOF, the parties hereto have caused this Addendum to be executed by their duly authorized officers effective as of the date first written above.

[COMPANY NAME]

By:
[Name] [Title]

DOTHAN CITY SCHOOLS

By: Dr. Chuck Ledbetter
Superintendent Dothan City Schools

Exhibit G:
Dothan City Schools FERPA Directory Information Disclosure

The Family Educational Rights and Privacy Act (FERPA), a Federal law, requires that the Dothan City Schools (District), with certain exceptions, obtain parents written consent prior to the disclosure of personally identifiable information from their child's education records. However, Dothan City Schools may disclose appropriately designated 'directory information' without written consent, unless parents have advised the district to the contrary in accordance with District procedures. The primary purpose of directory information is to allow the Dothan City Schools to include this type of information from their child's education records in certain school publications. Publications may be in print or digital format. Examples include, but are not limited to, the following:

- A playbill, showing a student's role in a drama production;
- The annual yearbook;
- Honor roll or other recognition lists;
- Graduation programs;
- Sports activity sheets, such as for wrestling, showing weight and height of team members; and
- School clubs.

Directory information, which is information that is generally not considered harmful or an invasion of privacy if released, can also be disclosed to outside organizations without a parent's prior written consent. Outside organizations include, but are not limited to, companies that manufacture class rings or publish yearbooks, take school pictures, or process data.

In addition, two federal laws require local educational agencies (LEAS) receiving assistance under the Elementary and Secondary Education Act of 1965 (ESEA) to provide military recruiters, and institutions of higher learning, upon request, with three directory information categories – names, addresses and telephone listings – unless parents have advised the LEA that they do not want their student's information disclosed without their prior written consent.
If parents do not want Dothan City Schools to disclose 'directory information' from their child's education records without their prior written consent, they must notify the school principal in writing within thirty (30) school days of the student's first day of attendance.

The District may disclose the following information as directory information:
- Student's name
- Address
- Telephone listing
- Electronic mail address

- Photograph
- Date and place of birth
- Major field of study
- Dates of attendance
- Grade level
- Participation in officially recognized activities and sports
- Weight and height of members of athletic teams
- Degrees, honors, and awards received

- The most recent educational agency or institution attended
- A student number assigned by the District (in some cases*)

* In order to make certain software applications available to students and parents, the District may need to upload specific 'directory information' to the software provider in order to create distinct accounts for students and/or parents. In these cases, the District will provide only the minimum amount of 'directory information' necessary for the student or parent to successfully use the software service.

Provisions for Consideration – Not Yet Implemented
Electronic Signature Agreement (Not Implemented)
[The following proposed agreement does not directly impact data security. But it could impact the outcome of challenges in cases where staff were asked to sign user agreements containing rules regarding data security electronically, but later protest that their digital signature was not valid.]
Dothan City Schools uses many types of electronic communications in order to conduct business. These include electronic mail, documents, applications, and forms. Digital formats enable the district to transmit information rapidly and to retain records efficiently. Throughout your employment with Dothan City Schools you will have occasion to use these various methods to make and respond to requests, convey and receive information, and electronically 'sign' forms and agreements.

Dothan City Schools may use a variety of methods to verify your electronic 'signature' or identity. These include: 1) submitting a form while logged into the network or software application under a password protected account and 2) submitting your employee id or social security number within a form along with other personal information that uniquely identifies you. Therefore, you must keep your network and software login ids and passwords secure at all times.
Agreement

I agree to maintain the security of the UserID and password assigned to me by Dothan City Schools in order to prevent disclosure of this information to anyone.
I agree that, if I have any reason to believe that the security of my UserID and password has been compromised, I will immediately inform the Technology Services department.
I agree that I will be held legally bound, obligated, and responsible for any submission I make in electronic format to Dothan City Schools as I would be by making such submission in hardcopy form with my handwritten signature as certification.
I understand that if I decline to use an electronic 'signature' for any particular communication or form, that I may be required to submit that form in a hardcopy form with a handwritten signature; and that is it my responsibility to inform the appropriate person that I am taking this action.
I understand that if there is a hardcopy versions and an electronic version of the same exact document, that the one that is most recent will be considered the binding document and that the handwritten document alone may not override the electronic version.

Section 8-1A-13 - Admissibility in evidence.

(a) In any proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.

(b) In determining the attribution and authenticity or evidentiary weight of an electronic record or signature, the trier of fact may consider, along with any other relevant and probative evidence, proof of the efficacy of any security procedure applied. This may include a showing that the procedure: (1) uniquely identifies the signer or creator of the record; (2) prevents others from using the same identifier; and/or (3) provides a mechanism for determining whether the data contained in the record was changed after it was created or signed. Evidence bearing on the means and the reliability with which the procedure performs these functions may also be considered.

Section 8-1A-5 - Use of electronic records and electronic signatures; variation by agreement.

(a) This chapter does not require a record or signature to be created, generated, sent, communicated, received, stored, or otherwise processed or used by electronic means or in electronic form.

(b) This chapter applies only to transactions between parties each of which has agreed to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties' conduct.

(c) A party that agrees to conduct a transaction by electronic means may refuse to conduct other transactions by electronic means. The right granted by this subsection may not be waived by agreement.

(d) Except as otherwise provided in this chapter, the effect of any of its provisions may be varied by agreement. The presence in certain provisions of this chapter of the words "unless otherwise agreed," or words of similar import, does not imply that the effect of other provisions may not be varied by agreement.

(e) Whether an electronic record or electronic signature has legal consequences is determined by this chapter and other applicable law.

Dothan City Schools

District Strategic Plan – Goals & Objectives

Strategic Goals and Objectives

Teaching and Learning

GOAL 1 Ensure that the curriculum and the delivery of the curriculum provides challenging, relevant, and equitable learning opportunities for all students.

Objective 1- Ensure that all course content and all course offerings are state aligned and the curriculum is locally approved.

Objective 2 - Ensure that pacing frameworks and common assessments are used throughout the district.

Objective 3 - Ensure that a research-based model for classroom instruction is used in every classroom throughout the district.

Objective 4 - Establish successful programs (and utilizing mentoring, peer tutoring, and community volunteers) to maximize student achievement for learners with diverse needs (academically at-risk, non-traditional, special needs, gifted, ELLs, Pre-K, etc.).

Objective 5 - Develop and increase professional conversations with teachers, classroom support staff, and administrators to improve classroom instruction.

Objective 6-Develop and improve practices to provide feedback to students and parents on standards-based progress, grade level progression, and post-secondary opportunities

GOAL 2 Collect, analyze, and use student achievement data for improved teaching and learning.

Objective 1 - Provide high quality professional development for teachers, instructional staff, and administrators on the effective use of data.

Objective 2 - Establish and maintain effective data collection and approved measures of student achievement to inform decision making by teachers, staff, parents, and students.

Objective 3 - Regularly monitor, evaluate and report student achievement data and its use in individual school continuous improvement plans and by other appropriate means.

Objective 4 - Use information gained through data analysis to guide instructional and budgetary decisions to improve student outcomes.

Objective 5 -Examine opportunities annually to add or enhance programs to improve student achievement when financially possible (expanded fine arts courses, additional and relevant Career Technical Education programs, early identification and intervention for At-Risk students)

Governance and Leadership

GOAL 1 Provide for qualified, effective, innovative Board of Education members.

Objective 1 - Provide on-going, high-quality orientation and training for Board of Education members.

Objective 2 - Review, revise and maintain effective Board of Education policies on which to base sound decision making, effective procedures, and fair consistent implementation of laws, rules, and guidelines.

Objective 3 - Board members should participate in school and community events that build positive community relationships.

Objective 4 - Board members should adhere to standards that entrust staff members with the day-to-day operations of the district.

GOAL 2 Provide qualified, effective, innovative system and school leaders.

Objective 1 - Recruit, employ, develop and retain highly qualified, effective, innovative system and school administrators.

Objective 2 - Provide on-going, effective, high quality professional development for the superintendent, system and school administrators.

Objective 3 - Encourage and support continuing education, part1c1pation in leadership development and attain credentials of distinction by system and school administrators.

Objective 4 - Encourage, support, and recognize administrator participation in local school and community events that build positive community relationships.

Objective 5 - Participate in programs of leadership development that prepare employees for possible future school and system level leadership.

GOAL 3 Provide opportunities to involve all stakeholders in collaborative efforts to improve school system governance.

Objective 1 - Establish and/or maintain advisory groups, councils, cooperative associations, booster clubs, and school support groups to include diverse representatives from all system stakeholders to provide input, feedback and ideas for improving school and system governance.

Objective 2 - Regularly collect, analyze, and disseminate summary information to system stakeholders on system accomplishments and data to guide their participation in decisions that will ensure that every student is successful.

Objective 3 - Collect and analyze public comments, suggestions, ideas and concerns about school system governance through surveys, correspondence, meetings and forums.

GOAL 4 Effectively use continuous improvement and accreditation monitoring plans to increase student achievement, to evaluate school system success, and to guide decision-making.

Objective 1 - Analyze, monitor, and evaluate all school and system continuous improvement plans at least annually and according to benchmarks identified in plans.

Objective 2 -Maintain system accreditation, utilizing the accreditation monitoring and reporting processes to promote and achieve continuous improvement toward system and school goals.

Objective 3 - Engage in regular orientation and trammg for school system personnel in the effective use of continuous improvement and accreditation plans.

Objective 4 - Regularly publish and report progress toward and accomplishment of school system strategic goals and accountability targets to all stakeholder groups.

Finance

GOAL 1 Dothan City Schools will practice responsible financial management and maintain appropriate financial reserves to support the critical instructional and operational needs of the system.

Objective 1 - Ensure that money is appropriated to schools based on state and federal guidelines.

Objective 2- Establish transparency among all schools as to how funds and resources are appropriated.

Objective 3 - Implement processes, controls and support systems to maximize operational efficiency and effectiveness

Objective 4 - Seek additional financial resources to support the successful implementation of all strategic plan initiatives.

Support Systems

GOAL 1 Dothan City Schools will implement effective programs and procedures to reduce school discipline incidents, suspensions, and expulsions.

Objective 1 - Provide safe, secure, inviting, and appropriate environments for a wide variety of extra-curricular and co-curricular activities.

Objective 2 - Review, update, and revise a system-wide code of student conduct and school safety plans on an annual basis.

Objective 3 - Develop a district culture of inclusion that is systemic, consistent, and equitable in intervening in conflicts and confusions arising from variations of differences.

Safety

GOAL 1 Dothan City Schools will provide support and professional expertise to schools as they create, enhance, and/or maintain safe, secure campuses.

Objective 1 - Identify schools with security needs and provide them with technical expertise.

Objective 2 - To establish a Culture of Safety through facilitation of family, school, and community engagement in shared responsibility and collaboration with community partnerships for positive outcomes.

Health

GOAL 1

Dothan City Schools will improve the overall mental health awareness and knowledge base of students and staff.

Objective 1 - Expand access to mental health and healthy practices through school-based and community partnerships to provide students with a well-balanced life.

Objective 2 - Provide employer assistance options to provide mental health services to staff.

Objective 3 - Maintain transitional support across all grades, between schools and from school to life.

Transportation

GOAL 1

Dothan City Schools will enhance and ensure the safe transporting of students to and from school on all system owned the school buses.

Objective 1- Acquire and utilize advanced technological resources.

Objective 2 - Streamline vehicle inspections and ensure adherence to safety policies.

Facilities and Maintenance

GOAL 1 Dothan City Schools will maintain facilities, services, and equipment to provide a safe, clean, and healthy environment for students and employees.

Objective 1 - Develop a long-term priority list of critical building needs including new construction, renovation and additions and deferred maintenance projects.

Objective 2 - Ensure that all school system facilities and campuses are clean, safe, attractive and well organized.

Technology

GOAL 1 Dothan City Schools will provide technology, infrastructure, essential equipment, and resources to support the instructional and operational needs of the system.

Objective 1 - Ensure that all classrooms have current, relevant and working technology.

Objective 2 - Examine opportunities to add or enhance technology to improve student achievement when financially possible.