



TECHNOLOGY PLAN 2022-2025

This document, and all contents included in the document, is the property of Eanes ISD. The district reserves the right to amend content included in the technology plan as needed. The Eanes ISD technology plan is not comprehensive of all district policies or procedures. The purpose of this plan is to provide structure and resources for staff in the application and use of technology, and as a communication tool for stakeholders regarding Eanes ISD technology initiatives. Duplicate with written permission only.

Introduction:

This technology plan includes historical and current information about the district, individual departments and technology implementations, and support models utilized across the district. During the development phase of this project, committee members identified a need to provide the academic community with foundational information about technologies available within the district, processes and procedures used by staff to ensure a safe and reliable experience for all users, and the variety of support and resources available to students and staff.

Information included in this document is evaluated and updated annually to reflect changes or additions to the infrastructure, classroom design or instructional needs.

Table of Contents:

| | |
|---|--------------|
| Background | Pages 4-5 |
| Board Priorities | Page 6 |
| Board Policies (Technology) | Page 7 |
| Technology Advisory Committee | Pages 8-9 |
| Technology Standards | Pages 10-13 |
| Roles & Responsibilities | Pages 14-17 |
| Responsible Use Guidelines (RUG) | Page 18 |
| Educational Technology <ul style="list-style-type: none"> • Teacher Support for Technology Integration • Student Support for Technology Integration • Digital Citizenship • Resource Vetting | Pages 19-31 |
| Technology Services <ul style="list-style-type: none"> • Elementary Green iPad • Web filters • Gaggle • iPad Protection Plan • Data Integration & Rostering • Textbook Adoptions • District Infrastructure • Systems & Applications | Pages 32-40 |
| Retirement Considerations | Page 41 |
| Guiding Principles | Page 42 |
| Goals & Objectives | Pages 43-48 |
| Future Planning | Pages 49-50 |
| Conclusion | Page 51 |
| References | Page 52 |
| Appendices | Pages 53-110 |

Background:

Eanes ISD is recognized as a national leader in educational programming. The District's instructional practices, technology integration and variety of course offerings are exemplary in the area of K-12 public schools. Meeting each student's needs is a primary goal of Eanes ISD. A comprehensive curriculum and a variety of enrichment opportunities are offered to EISD's students, including proudly serving as a 1:1 mobile device district since 2012. In 2019 the community of Westlake supported the district by passing a bond proposal providing funding and resources to update classroom technologies, student and staff devices, and hardware/software to support infrastructure including wired and wireless networks.

The District is comprised of 9 school campuses:

| Elementary Campuses | Middle School Campuses | High School Campuses & Programs |
|---|--|---|
| Barton Creek Elementary | Hill Country Middle School | Westlake High School |
| Bridge Point Elementary | West Ridge Middle School | Adult Transition Services |
| Cedar Creek Elementary | | |
| Eanes Elementary | | |
| Forest Trail Elementary | | |
| Valley View Elementary | | |

Thoughtful Use of Technology: Eanes ISD believes technology is the intentional, purposeful integration of developmentally appropriate digital tools, materials, and knowledge used to enhance student engagement and learning for everyone in our learning community. We believe technology enhances opportunities for differentiation, creation, collaboration, critical thinking, and digital citizenship.



In order to accomplish the desired outcomes for students, and further the district's investment in technology and professional development opportunities for staff, this technology plan emphasizes

the continued need for the necessary infrastructure, tools, and proficiencies that will be required to achieve the goals and objectives of this multi-year technology plan.

Elements identified in this plan will require continued funding from both the district and possible bond proposals.

This technology plan includes an overview of the processes and procedures currently utilized by the district to ensure the academic community has a technology-rich, reliable, and secure environment for all users. Goals and objectives identified in this document will serve as a foundation for technology systems for future bond proposals.

Board Priorities:

2021-22 School Year: Each year the Board of Trustees identifies district goals and priorities for each of the departments within the district. The areas of focus for the board priorities include the following areas:

| | |
|----|--|
| 1. | Instructional Priority: A Culture of Guaranteed Viable Curricula (GVC) |
| 2. | Instructional Priority: Diversity Equity and Inclusion |
| 3. | Instructional Priority: Student Support |
| 4. | Operational Priority: Staff and Community Engagement |
| 5. | Operational Priority: Operations and Long-Range Planning |

This technology plan, as designed by the Technology Advisory Committee, consists of information and goals that align with both the instructional and operational priority areas. Full details of the board priorities can be found [here](#). Technology Services, categorized under Operations and Long-Range Planning, was charged with implementing the following operational goals:

- **Maintain a long-range plan for operational processes**
 - Study potential budgeting and policy priorities as a result of, or in preparation for, legislative priorities
 - Analyze demographic, enrollment and transfer data to optimize resources, facilities and staffing
- **Safeguard students, staff and resources by securing schools and cyber technologies**
- **Examine and re-evaluate budget priorities in preparation for or in response to evolving circumstances**
 - Continue a multi-year strategic budgeting approach
 - Manage capital projects and plan for possible future bonds with community input
 - Explore collaborative or alternative fundraising and revenue generation strategies

Board Policies: Technology

Eanes ISD maintains and refers to policies governing the operation of this District. The policies were created:

1. because they are required by law or by the Texas Education Agency;
2. because they are recommended by the Texas Association of School Boards as essential to effective District governance and management; or
3. because the Board wishes to make a statement in a particular policy area.

Eanes ISD has numerous board policies related to technology use and application within the district. District and campus administrators refer to these policies for guidance when technology-related scenarios arise. A full list of board policies can be found [here](#). See *appendices A, B & C*.

Technology Advisory Committee:

The purpose of the Technology Advisory Committee (TAC) is to provide input, guidance and support for district technology initiatives. The TAC membership is composed of Eanes ISD parents, students, teachers and administrators. The committee membership offers a diverse perspective on technology integration, data privacy and instructional expectations for the *Thoughtful Use of Technology*.

Advisory Committee members serve as representatives of their respective areas to provide input and guidance to district leaders. As part of their commitment to the district's work, the TAC members were given the following charges:

- Identify and articulate developmentally appropriate practices for integrating technology into classroom instruction, such as thoughtful use, technology integration, and screen time.
- Provide input and articulate technology-focused themes for the district's technology plan.
- Review the district's cybersecurity and data privacy procedures and risk management processes.
- Provide input into the selection process of a K-12 learning management system.

Benchmarking: In preparation for the creation of this technology plan, TAC members researched and evaluated plans from multiple K-12 Texas school districts to identify best practices, exemplar plans, user-friendly formatting and style. The table below includes the benchmarking districts reviewed during the research and development phase of this plan.

| | | |
|-----------------------------------|---------------------------------|--------------------------------|
| Dallas ISD | Fort Bend ISD | Fort Worth ISD |
| Highland Park ISD | Lake Dallas ISD | Plano ISD |
| San Antonio ISD | | |

Committee Members:

Thank you to committee members who served during the 2020-21 & 2021-22 school years. Each member provided feedback and support to the Educational Technology & Technology Services teams. The current committee members are included below.

| | |
|--------------------|--|
| Nancy Abell | Elementary Gifted & Talented Teacher |
| Fred Benitez | Director Educational Technology |
| Loren Boyd | High School Educational Technology |
| Anne Buchta | Special Education - Assistive Technology |
| Dianne Carter | Middle School Administrator |
| Katie Dawkins | Middle School Science Teacher |
| Susan Fambrough | Chief Learning Officer |
| Abigail Frederick | Community Member |
| Braden Herring | Director Technology Services |
| Jacquelyn Johnson | Community Member |
| Jay Kamm | Community Member |
| Holly Leicht | Middle School Educational Technology |
| Erin Levy | Elementary Gifted & Talented Teacher |
| Safina Mahmood | Community Member |
| Madiha Marium | Middle School Educational Technology |
| Kelly Marwill | Community Member |
| Katie Poole | Elementary Teacher |
| Kara Predatsch | Middle School Teacher |
| Kate Richter | Elementary Librarian |
| Marianna Ricketson | Elementary Educational Partner |
| Charles Riley | Community Member |
| Dr. Kristy Sailors | Chief Technology Officer |
| Bill Wiese | Community Member |
| Laura Wright | Elementary Art Teacher |
| Andrew Z. | High School Student |

Technology Standards:

Eanes ISD utilizes the State of Texas TEKS ([Texas Essential Knowledge and Skills](#)), based on the ISTE ([International Society for Technology Education](#)) standards, to develop instructional activities that are embedded with technology application expectations/skills for students in grades K-12. Educators in our community believe that technology can be thoughtfully and effectively integrated into all subject areas and view technology as a tool used to enhance other instructional methods and learning materials. *See appendix H.*

Additionally, Eanes ISD is bound to follow the guidance and priorities identified and presented by the long range plan developed and published by the Texas Education Agency (TEA). Components of the TEA long range plan are included on the next pages.

Texas Education Agency - Long Range Plan for Technology (2018-2023)

As identified in the [Long Range Plan for Technology \(2018-2023\)](#), Texans want a system of public education that is equitable, accessible, and staffed by skilled educators and that offers opportunities for students that will carry them through school and into college, careers, or the military. Today's students will be tomorrow's citizens and workforce, so ensuring that our young people are well educated is critical for the state to have a stronger future. An effective education system is key to equipping students with the knowledge, skills, and integrity to contribute to our state in positive ways. Technology is a driving force for transforming education as we know it, creating stronger, better-educated students, and ultimately building a stronger Texas.

Included in the TEA Long Range plan for Technology, are six strategic goals with defined areas of focus under each. These strategic goals are a foundation for technology-based initiatives for all Texas K-12 institutions. The strategic goals, developed by TEA, are included on the next pages of this document.

The table below reflects the strategic goals as identified by TEA's long range technology plan. The full TEA plan can be found [here](#).

| TEA Strategic Goal 1 - Personalized, Flexible, Empowered, Learning Environment (see page D-8): |
|---|
| <ul style="list-style-type: none"> Implementing a successful personalized learning practice requires a whole new way of thinking about education. |
| <ul style="list-style-type: none"> Imagine an education system where students move at their own pace, have the freedom to make decisions about their own learning, and adapt lessons to their own interests, abilities, and style. A system where students are engaged and motivated, and progress is inherently assessed along the way. |
| <ul style="list-style-type: none"> Students no longer need to be bound by traditional classroom space or by traditional learning methods. Data can be used to present the right lessons at the time most needed. |
| <i>Focus Areas for Goal 1: Student-Centered & Adaptive; Reimagined Learning Spaces; Data-Driven Decisions</i> |

| TEA Strategic Goal 2 - Equitable Access (see page D-10): |
|---|
| <ul style="list-style-type: none"> Preparing all students for success in the 21st century and ensuring that all students have the technology skills to fully participate and thrive in the world is a top concern for all educators. |
| <ul style="list-style-type: none"> Technology provides opportunities to transform education, but only if all students can fully participate. When implementing technology, it is important to consider not only the number and type of technology devices you need but also how to connect them, how to use them, and how to leverage available digital resources to meet learning and teaching goals. |
| <i>Focus Areas for Goal 2: One-to-One (1:1) Initiative; Connectivity; Usability</i> |

TEA Strategic Goal 3 - Digital Citizenship (see page D-12):

- As digital resources become more prevalent so does the need for greater digital responsibility.
- Each student must become aware of their own ability to make effective choices and the impact that has on the world around them and for themselves in reaching their full potential.
- Educators and parents have a joint responsibility in teaching the components of respect, education, and protection in a digital world.

Focus Areas for Goal 3: Program Development; Content Development; Rights and Responsibilities

TEA Strategic Goal 4 - Safety and Security (see page D-14):

- The safety of every student on every campus is a top priority for everyone in Texas. School safety continues to be in the forefront of the discussion and encompasses many issues and strategies to better prepare and protect students and staff.
- LEAs are obligated to provide secure and reliable information and services to both the students they serve and the workforce they support. The amount of information created and stored is growing exponentially. As the need to provide access to information grows, the public sector continues to be an attractive target for cybersecurity attacks.

Focus Areas for Goal 4: Cybersecurity; Campus Safety; Data Management and Governance

TEA Strategic Goal 5 - Collaborative Leadership (see page D-16):

- With so many challenges facing organizations and so many priorities competing for resources, educators need to find ways to do more with less and to work smarter, not harder.
- Given the existing budget and resources constraints, LEAs must prioritize their goals, have a clear, unified vision for achieving those goals, and look for collaborative, cost-effective solutions. Having all stakeholders on board is critical to accomplishing the most with resources available.

Focus Areas for Goal 5: Strategic Planning; Shared Services; State Collaboration

| |
|--|
| TEA Strategic Goal 6 - Reliable Infrastructure (see page D-18): |
| <ul style="list-style-type: none"> • LEAs are facing the challenge of modernizing legacy hardware and software, replacing aging systems to move toward a more collaborative, agile, and interoperable education system. |
| <ul style="list-style-type: none"> • As LEAs transition from traditional practices to innovative solutions, they need to evaluate current and ongoing investments in legacy systems and hardware while considering replacement with more efficient and scalable options. |
| <ul style="list-style-type: none"> • As more and more learning opportunities rely on technology to enhance educational experiences, a reliable infrastructure is critical for LEAs to obtain their educational goals. Determining what equipment and support is needed, by whom, and how to get there may not be easy, but it is essential to the future success of educational IT. |
| <i>Focus Areas for Goal 6: Technical Support; Legacy Modernization; Continuity of Operations</i> |

Eanes ISD will refer to the TEA strategic goals as a reference for the technology related initiatives and planning. The goals and objectives included in this plan are reinforced by the goals identified by TEA.

Roles and Responsibilities:

The Technology Advisory Committee (TAC) believes that everyone in the Eanes academic community has a responsibility to provide an educational environment that fosters learning for all students. To further this belief, TAC identified the following responsibilities in regards to student learning with technology:

| Roles & Responsibilities |
|---|
| <p>In the area of educational technology, the BOARD OF TRUSTEES are responsible for:</p> <ul style="list-style-type: none">• Providing guidance, setting policy and identifying resources and funding to support technology initiatives.• Identifying policies that determine district technology processes and align with the district's vision for <i>Thoughtful Use of Technology</i>.• Providing District Administrators with direction and governance for the district's mission which can be supported by the technology team.• Directing District Administrators to make changes to policies based on community input.• Supporting Campus and District Leadership and other staff who are fulfilling their responsibilities as listed above.• Approving the district's technology plan. |
| <p>In the area of educational technology, DISTRICT LEADERS are responsible for:</p> <ul style="list-style-type: none">• Providing the infrastructure and support for technology utilized in the district.• Providing processes and guidance for purchasing and implementing technology tools.• Monitoring safety and data privacy for students and staff when utilizing technology tools.• Identifying and evaluating digital resources to ensure alignment with district initiatives.• Providing professional learning for staff that assists them with technology-rich instructional design concepts.• Promoting the importance of <i>Thoughtful Use of Technology</i> as part of the instructional day, balancing technology use with other instructional methods.• Developing curriculum and curriculum-aligned learning experiences that teach students to be effective, responsible users of technology related to the technology TEKS and are reflective of future learning landscapes beyond school (i.e., college and career).• Ensuring parents, students, teachers and staff are aware of their rights regarding the use of educational technology and digital materials.• Partner and cooperate with law enforcement and security professionals, following district policies and procedures, in the event of a cybersecurity event or threat.• Defining and maintaining current Responsible Use Guidelines and code of conduct that will be used throughout the district. |

Roles & Responsibilities

In the area of educational technology, **TECHNOLOGY SERVICES STAFF MEMBERS** are responsible for:

- Following best practices for safety protocols, providing secured, reliable networks (wired and wireless) that are accessible to the academic community.
- Administering and monitoring systems and applications to provide ease of use and access for the academic community.
- Safeguarding district provided devices, systems and resources.
- Serving as the primary point of contact for security incidents or data breaches.
- Being responsive to the needs of the academic community as it relates to technology applications, instructional use, and thoughtful integration.
- Partnering with campus, technology advisory committee and district administrators on all district initiatives.
- Providing a flexible learning environment appropriate for individual users.
- Developing long range plans targeting state of the art technologies, infrastructure and applications to meet the evolving needs of learners.
- Maintaining and repairing classroom technologies.

In the area of educational technology, **CAMPUS LEADERSHIP TEAM MEMBERS** are responsible for:

- Monitoring safety and data privacy for students and staff when utilizing technology tools.
- Supporting and providing professional learning for staff that assists them with technology-rich instructional design concepts.
- Overseeing curriculum and learning experiences that teach students to be effective, responsible users of technology related to the technology TEKS and are reflective of future learning landscapes beyond school (i.e., college and career).
- Promoting the importance of *Thoughtful Use of Technology* as part of the instructional day balancing technology use with other instructional methods.
- Monitoring, evaluating and supporting effective instructional use of educational technology in classrooms that enhance traditional teaching methods and support the curriculum standards.
- Advocating and addressing campus technology needs.
- Partnering with district staff on various initiatives involving technology.
- Communicating with Technology Services on upcoming campus events and technology needs.

Roles & Responsibilities

In the area of educational technology, **EDUCATIONAL PARTNERS and EDUCATIONAL TECHNOLOGISTS** (EPs/EdTechs) are responsible for:

- Monitoring safety and data privacy for students and staff when utilizing technology tools.
- Providing professional learning for staff that assists them with technology-rich instructional design concepts.
- Promoting the importance of *Thoughtful Use of Technology* as part of the instructional day balancing technology use with other instructional methods.
- Supporting curriculum and curriculum-aligned learning experiences that teach students to be effective, responsible users of technology related to the technology TEKS and are reflective of future learning landscapes beyond school (i.e., college and career).
- Supporting staff and students in their application of educational technology and digital citizenship.
- Partnering with Curriculum and Instruction staff to provide instructional resources and support based on campus/district goals and priorities.
- Designing instructional activities and lessons, relying on UDL and SAMR frameworks, to engage students in the learning process.
- Delegating to the Technology Services staff for hands-on hardware support.

In the area of educational technology, **TEACHERS AND LIBRARIANS** are responsible for:

- Monitoring safety and applicable data privacy for students when utilizing technology tools when in the classroom or other instructional setting.
- Continually monitoring student use of technology in the classroom.
- Engaging in professional learning for staff that assists them with technology-rich instructional design concepts.
- Utilizing technology when it is determined to be the best tool for teaching the instructional objectives.
- Teaching technology-related curriculum and designing curriculum-aligned learning experiences that teach students to be effective, responsible users of technology as per the technology TEKS and are reflective of future learning landscapes beyond school (i.e., college and career).
- Promoting the importance of *Thoughtful Use of Technology* as part of the instructional day balancing technology use with other instructional methods.
- Designing instructional activities and lessons, relying on UDL and SAMR frameworks, to engage students in the learning process, partnering with Educational Partners as needed.

Roles & Responsibilities

In the area of educational technology, **PARENTS and/or GUARDIANS** are responsible for:

- Reviewing the [Responsible Use Guidelines](#) for their children during the registration process. Parents/Guardians should ensure their children understand the terms of the policy.
- Understanding and helping their students adhere to the [code of conduct](#) and responsible use guidelines as accepted during student registration.
- Providing guidance to their children to support the balance of instructional use and recreational use of technology to support positive digital citizenship.
- Partnering with teachers and campus administrators to support students with online safety, self regulation and managing digital distractions when using district or personal devices.
- Remaining knowledgeable and aware of district-provided safeguards and partnering with the district's technology services department and campus staff to provide additional safeguards to student devices and accounts.

In the area of educational technology, **STUDENTS** are responsible for:

- Following the district's [Responsible Use Guidelines](#) for appropriate use of district's technologies, resources and wired and wireless networks, which are reviewed annually with each student.
- Ensuring their device is available, charged and ready to use in the classroom.
- Using best practices for online safety including email, websites and district provisioned accounts.
- Safeguarding district provided devices and resources.
- Following classroom rules and procedures as determined by teachers and administrators.
- Using the device to further the educational and administrative purposes, academic goals, and learning objectives of Eanes ISD.
- Following the student code of conduct or employee standards of conduct.
- Following copyright rules and properly citing websites, content, and media for instructional activities and research.

Responsible Use Guidelines:

Technology is essential to facilitate the creative problem-solving, information fluency, communication and collaboration required in the global economy. The Responsible Use Guidelines (RUG) support the district's vision of responsible technology use and promotes a strong sense of digital citizenship. The RUG applies to all Eanes Independent School District computer networks (including the devices made available by them), and all devices connected to those networks (whether they be staff-owned or otherwise).

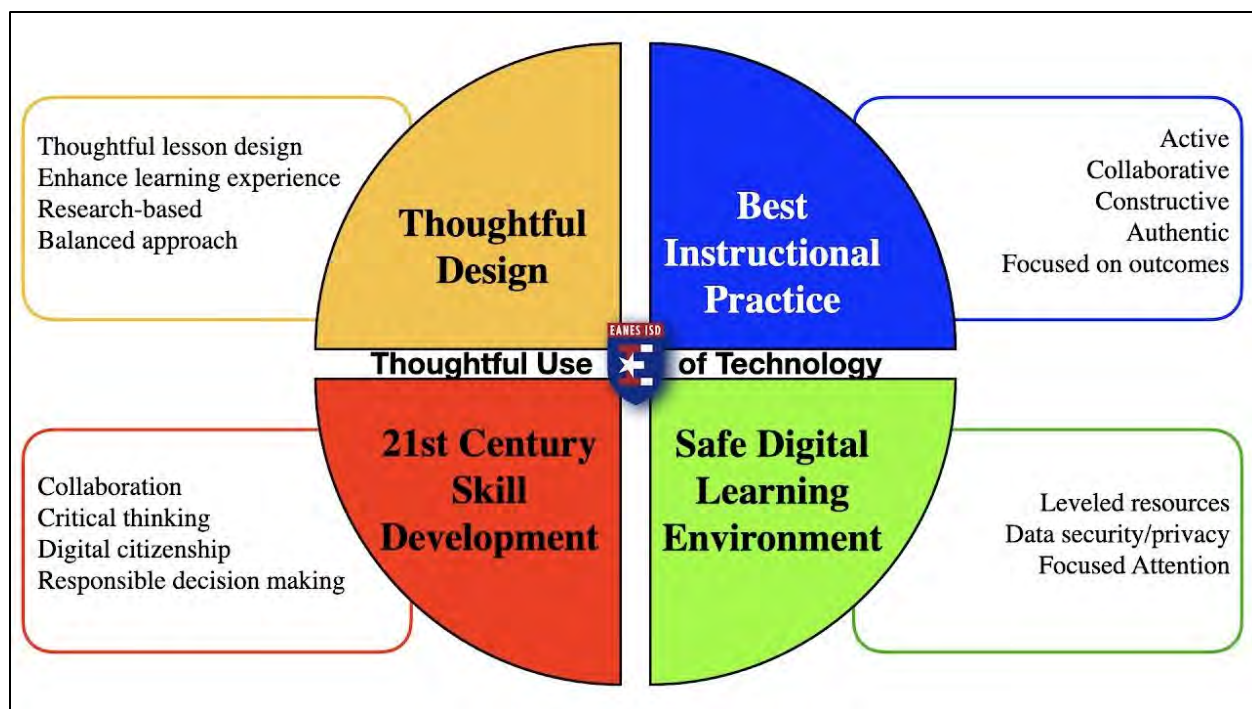
The district maintains Responsible Use Guidelines for students (grades K-12) and staff. A full list of the RUGs are linked below. The RUGs are updated and reviewed annually with students and staff members to confirm understanding and to set expectations for responsible and appropriate behavior. Updated copies of the Responsible Use Guidelines can be found [here](#). See *appendices D, E, F & G*.

- [2021-22 Teachers and Staff RUG](#)
- [2021-22 Elementary students RUG](#)
- [2021-22 Middle School students RUG](#)
- [2021-22 High School students RUG](#)

Educational Technology:

The [Educational Technology Team](#), under the leadership of the Director of Educational Technology, is responsible for the expansion of technology integration and supporting teachers in the understanding and application of appropriate and *Thoughtful Use of Technology*. Decisions and recommendations for technology integration in Eanes ISD align with the district's belief around the *Thoughtful Use of Technology*, relying on educational and technology integration frameworks.

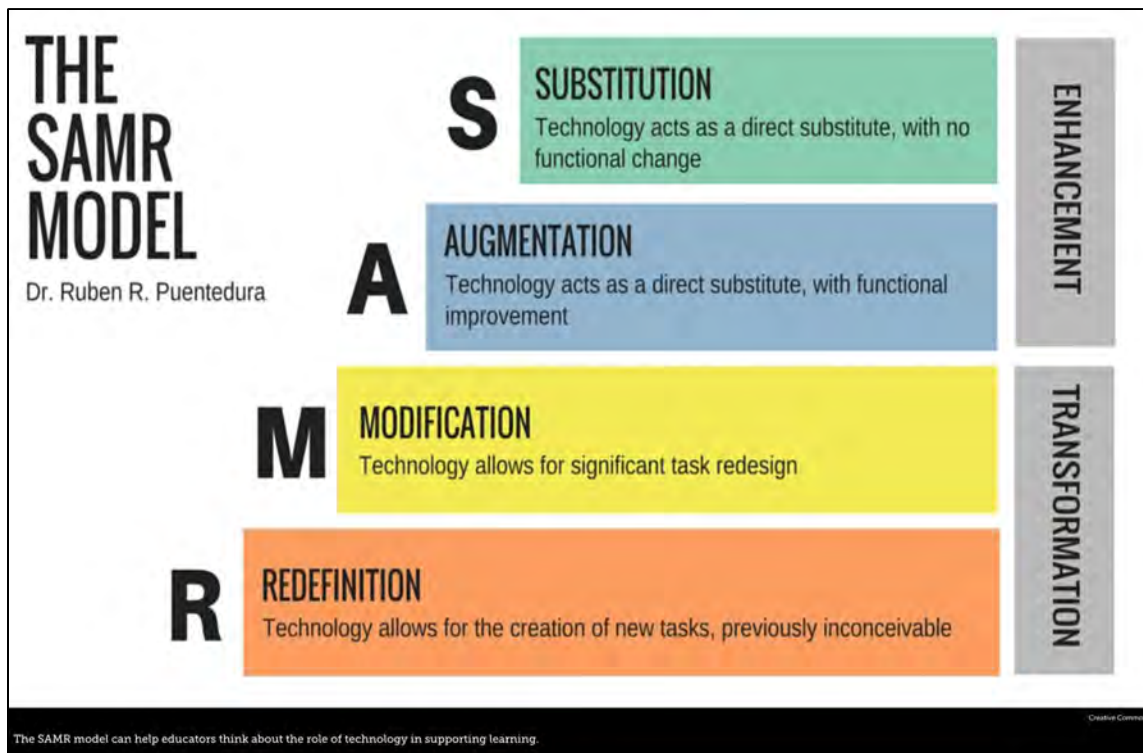
As the district developed the concept and belief of the *Thoughtful Use of Technology*, teachers and staff were able to see an alignment with other elements of the EISD planning framework. The District believes *Thoughtful Use of Technology* begins with lesson design. As teachers design lessons, we ask them to utilize the EISD planning framework to ensure technology integration is purposeful, enhances the learning experience and aligns to our Texas Essential Knowledge and Skills (TEKS). The EISD planning framework is included below.



Teacher Support for Technology Integration:

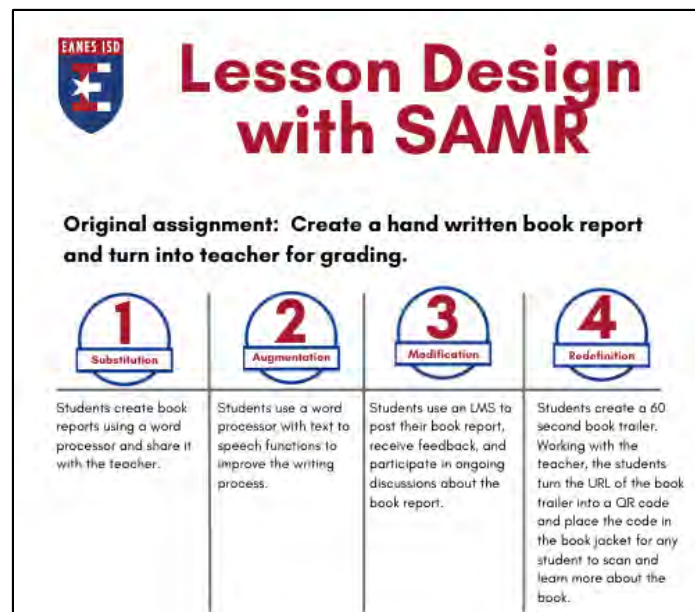
SAMR: [Dr. Ruben Puentedura](#) developed the SAMR model as a reference for teachers to evaluate how they are incorporating technology into instructional practices. The SAMR model consists of four tiers, presented roughly in order of their transformative power: (S) substitution, (A) augmentation, (M) modification, and (R) redefinition. When educators reflect upon how they are integrating technology into the classroom it is tempting to think of SAMR as a mountain to be summited. But educational technology integration is not about getting to or remaining at the top of the SAMR model; it is about being aware of the range of options and picking the correct strategy needed for the learning objectives.

The original SAMR model, as created by Dr. Puentedura demonstrates a stair step approach to using technology by enhancing lesson design to actual transformation of the student product. The original SAMR model is included below.



To better understand how technology can be utilized in classrooms and the effectiveness of technology integration, the district identified the SAMR model as a framework that best demonstrates multiple layers of technology use. Eanes ISD selected SAMR as the instructional framework during the original 1:1 implementation in 2013. This [technology integration model](#) best aligns with the beliefs and instructional practices in the district. During lesson design, and referring to the [Eanes ISD SAMR model](#) and [Eanes ISD SAMR Flowchart](#), teachers can evaluate technology use by responding to these questions:

- **Where does my lesson fit within the SAMR framework?**
- **How am I going to teach this and see evidence of student learning?**
- **Can technology help to get all students equitable access to meaningful learning?**



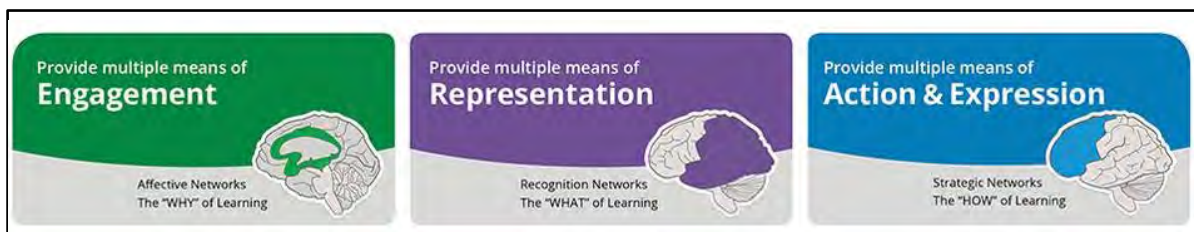
To further explain how the SAMR model can transform student products, Eanes ISD staff developed an infographic altering the student product through the stages of SAMR. The above image is an example of how the SAMR model transforms the student product using the original assignment. See *appendices I, J & K*.

UDL: Universal Design for Learning (UDL) is an educational framework that was developed and promoted by CAST (<https://udlguidelines.cast.org/>) as a resource for teachers and administrators when designing lessons and instructional activities. These guidelines offer a set of concrete suggestions that can be applied to any discipline or domain to ensure that all learners can access and participate in meaningful, challenging learning opportunities.

Applying the UDL design principles allows teachers to create instructional activities that are accessible to all learners and meets them at their individual level. Using UDL concepts, learners are presented with the information in a variety of formats that allows the student to select the format that best meets their unique learning style and preferences - providing true personalized learning for all.

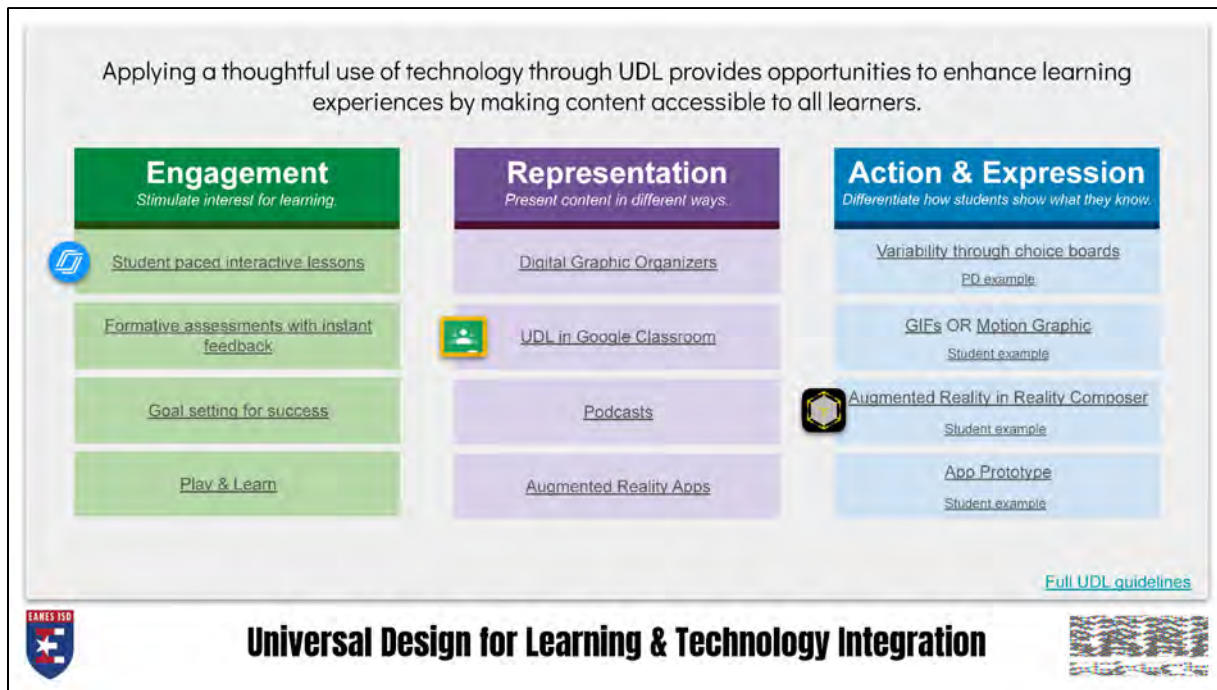
UDL concepts used by teachers in the district include the following options:

- Adding visual elements such as graphics and colored text for improved visibility for students.
- Providing the same content in a variety of formats, such as tables, graphs, images and audio enhancements allowing students to process the content using their personal learning preferences.
- Incorporating captioning on videos to improve understanding and leveled access for students who may need visual prompts for comprehension.



CAST (2018). Universal Design for Learning Guidelines version 2.2. Retrieved from <http://udlguidelines.cast.org>

Teachers in Eanes ISD utilize UDL concepts to design instructional materials and lessons incorporating multiple delivery methods and styles to ensure students are exposed to the content in a format that best meets their learning needs. Below is a sample choice board, designed using UDL concepts and focusing on technology integration. The fully interactive sample can be found [here](#). See *appendix L*.



This choice board example provides options for students when making selections about the activity or type(s) of technology they would like to use to demonstrate their learning. Providing students with choices empowers them to use technologies to alter traditional homework submissions and transforms their learning experiences. When planning, teachers can refer to the [Eanes ISD Technology Through UDL](#) infographic.

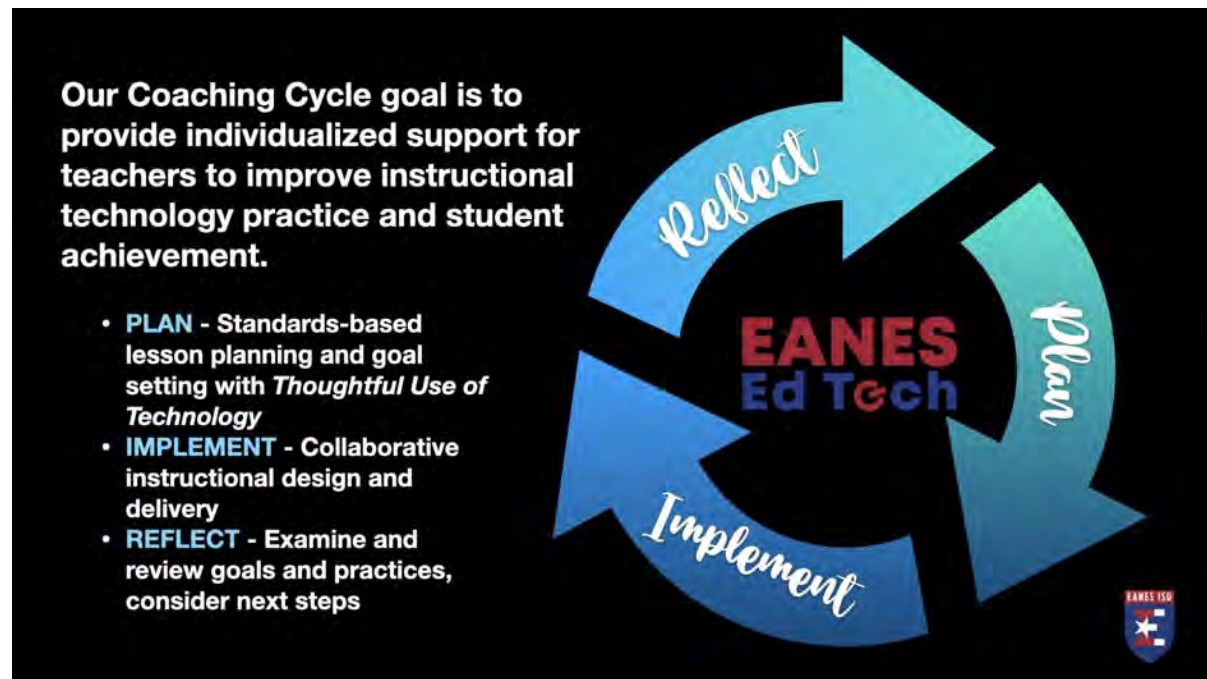
Instructional Rounds: Instructional Rounds are a non-evaluative opportunity to collect real-time feedback on teaching and learning in the classroom. [Through the lens of UDL](#), Eanes ISD Educational Technology personnel use data collected during Instructional Rounds to identify areas of need for professional development related to the *Thoughtful Use of Technology*. Additionally, the Technology Educational Partners conducted “Virtual Instructional Rounds” via Google Classroom to gather information about the different learning and teaching styles offered to students through our learning management system.

Professional Development:

Tech Playbook - Eanes ISD is an Innovative School District with rich technology integration and support for student experiences. The resources provided in the [Tech Playbook](#) provide a foundation for understanding technology integration to support and enhance their instructional approach.

New Teacher Support - Throughout the school year, teachers new to the profession and new to the district will be provided with ongoing support from assigned mentors and campus Educational Partners. This partnership will focus on best instructional practices, campus culture and *Thoughtful Use of Technology* through collaborative experiences, peer observations, and modeling.

Coaching Cycles - Educational Partners in Eanes prioritize the growth and development of teachers. Our Eanes Ed Tech goal is to increase the achievement and engagement of every student through the *Thoughtful Use of Technology*. We are committed to teacher growth and support through coaching cycles.



Summer Professional Learning - Educational Partners provide a variety of professional learning opportunities for Eanes ISD staff. Professional development sessions are offered in person and asynchronously via Google Classroom. Ed Tech's provide Universal Design for Learning and SAMR focused instructional frameworks for asynchronous courses and have developed a template for delivery and course design.


Student Support for Technology Integration:

Student Onboarding - Eanes ISD Students are onboarded with technology in a way that is developmentally appropriate for them and incorporating the device they will utilize as part of their learning. In aligning with a safe digital environment, the district implemented a Green iPad at the elementary level. The Green iPad configuration contains instructionally focused apps, evaluated by teachers to ensure alignment with curricular objectives. Each mobile app is also evaluated for alignment with the district's guidelines for student data, privacy and security.

At the secondary level, student iPads have less restrictions than elementary students, and are able to access a variety of district approved applications through the Student App. In 6th grade, students are enrolled in a technology class for one-third of the school year. In this course, students learn about digital citizenship, keyboarding skills and basic technology applications (word processing, presentation, spreadsheets, etc). Sixth graders also participate in the "Tech Rally" at the beginning of the year which helps them with productivity such as checking grades, setting up email, subscribing to teacher calendars, etc. At the high school level, incoming freshmen participate in an "iPad Base Camp" presentation that includes breakout sessions on the instruction and technology resources provided to them.

Digital Citizenship - Eanes ISD uses the *Thoughtful Use of Technology* as one way of enhancing the mission to prepare and inspire all students for life-long success by teaching the skills, knowledge and behaviors students will need as responsible citizens in the global community. Digital citizenship is embedded in daily teaching and learning within the 1:1 iPad environment. Eanes ISD is committed to fostering technology integration that promotes well-being and safe practices for students, staff, and families.

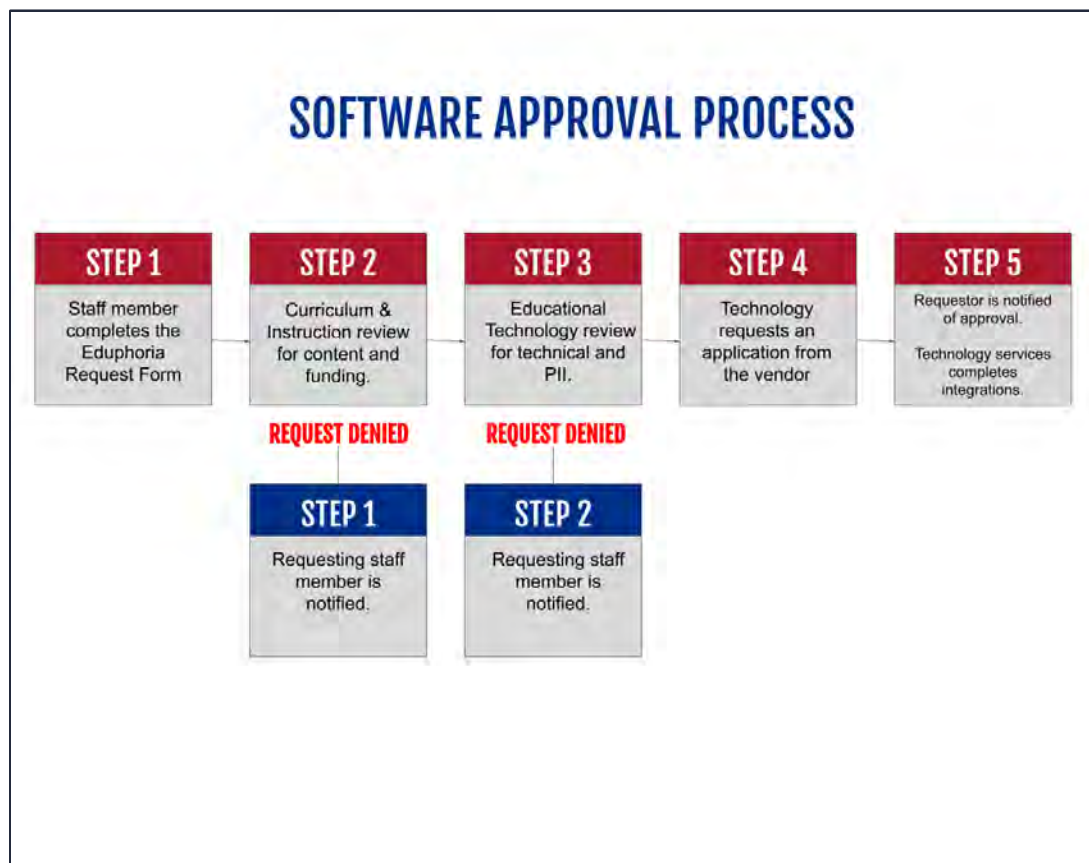
Resource Vetting Process: To better align the evaluation, vetting, and selection processes for mobile apps and digital resources, the district utilizes a detailed rubric to be used to complete thorough and consistent evaluations. The multi-step evaluation rubric is included below and allows district staff to score resources using elements such as academic relevance, data privacy, ease of use and mobile management. This evaluation rubric is referenced when selecting either purchased or free resources.



Eanes ISD - Internal Evaluation Rubric

| Components | 1 | 2 | 3 | Score |
|--|---|--|---|-------|
| Acceptable Use/Privacy Statement <ul style="list-style-type: none"> • COPPA/CFR/FERPA compliant • Account requirements • Data sharing and collection • Third-party applications login • Parental consent required | Terms of use or privacy statement is unclear or contains minimal information pertaining to staff or student PII. | Terms of use or privacy statement contains basic information pertaining to staff or student PII. | Terms of use or privacy statement contains detailed information pertaining to staff or student PII. | |
| Age Requirements or Parental Consent <ul style="list-style-type: none"> • Does the resource have age restrictions? • Does the resource require parental consent? | The resource has minimum age requirements or requires parental consent. | The resource has recommended age requirements but does not require parental consent. | The resource does not have age requirements or requires parental consent. | |
| Social appropriateness and/or educational relevance <ul style="list-style-type: none"> • Content is of educational quality • resource aligns with classroom instruction | Content is inappropriate for K-12 students. | Content has some questionable material but can be managed through login. | Content is appropriate for K-12 students. | |
| User Generated Content <ul style="list-style-type: none"> • Content contains appropriate information (images, text, URLs) • Can anonymous individual comment on others work? • Can the comments or chat be monitored? | The resource contains built-in search features and opportunity for inappropriate content. | The resource requires account to use built-in search features and limits inappropriate content. | The resource does not contain built-in search features and no inappropriate content is visible. | |
| Feedback <ul style="list-style-type: none"> • The resource provides students with feedback or encouragement? • Feedback is inappropriate for students | The resource does not provide user with feedback. | The resource provides user with minimal feedback. | The resource provides user with leveled feedback. | |
| Leveled Customization <ul style="list-style-type: none"> • Can teachers adjust the settings for individual student needs? | Settings do not allow for customization or differentiation options. | Settings have minimal customization options. | Settings are fully customizable for users. | |
| Usability of Interface <ul style="list-style-type: none"> • Will the teacher have to spend time teaching the students how to use the resource or is it easy to learn? | Students will need assistance navigating the resource. | Students are able to navigate the resource with minimal guidance. | Students are able to navigate the resource without assistance. | |
| Communication Features <ul style="list-style-type: none"> • Does the resource have a built-in chat feature? • Can the chat or discussion posts be moderated/archived by the teacher? | The resource contains the option for anonymous communication. | The resource contains the option for monitored communication. | The resource contains the option for monitored communication and archiving. | |
| Advertisements <ul style="list-style-type: none"> • Are the ads static or do they change depending on time of day? • Are the ads placed on the content area? | The resource contains intrusive ads or the placement of the ads blocks content. | The resource is static and does not block content. | The resource does not contain ads. | |
| Accessibility Features for Special Needs <ul style="list-style-type: none"> • Are there settings that support students with vision/hearing limitations? • Are there settings that allow users to adjust colors or text? • Are there settings that allow users to have text read to them? | The resource contains no accessibility features. | The resource contains minimal accessibility features. | The resource contains multiple accessibility features. | |
| Data Encryption <ul style="list-style-type: none"> • Enter site website into the search field at www.ssllabs.com to view security "grade" | Data is not safe in transit (Received grade of "D" or "F" on www.ssllabs.com .) | Data is protected, but the key exchange is weak (Received a grade of "C" on www.ssllabs.com .) | Data is completely encrypted in transit (Received grade of "A" or "B" on www.ssllabs.com .) | |
| Additional Components | (ES/NO) | | | |
| Does the resource contain built-in purchases? | | | | |
| Is the resource MOA compliant? | | | | |
| Is the resource free or require purchase or subscription? | | | | |
| Does the resource contain Google integration? | | | | |
| Total Score (33 points possible): | | | | |

Software approval process: Ensuring district staff and departments are evaluating and selecting software applications that are appropriate and align with the district's standards for data privacy and security. The district adheres to a software approval process. Throughout the process, various staff members rely on rubrics and standards to evaluate the software request for potential purchasing. In addition to curriculum alignment and privacy standards, departments review available funding sources for potential purchases. The software approval process is included below.



When determining which software applications or subscriptions are continued, the district utilizes annual usage reports, licensing compliance and budgetary restrictions. Any application, regardless of installation method, that is terminated from the resource inventory, district staff references the procedures included in the vendor agreement application for termination and data destruction.

Data Sharing Addendum: Aligning with best practices and emphasizing student safety, Eanes ISD has identified a workflow for the procurement of technologies and digital resources, including the requirement for vendors to complete the district's data protection addendum (DPA) addressing processes and procedures for handling student and staff data. The DP

A outlines the processes and procedures as it relates to the collection, management and protection of student data throughout the life of the contract and includes requirements for secure destruction upon termination of the contract or services. The image below includes the vendor approval process and steps completed by district staff throughout the procurement process. A copy of the district's DPA, software agreement and vendor packet can be found in the appendix section of this document. See *appendices O & P*.



TrustED App Dashboard: During the 2021-22 school year, the district partnered with [IMS Global Learning Consortium](#) to provide additional resources and apply data security measures for students and staff. The partnership with IMS Global provided the district with additional support, resources and security measures when evaluating digital resources.

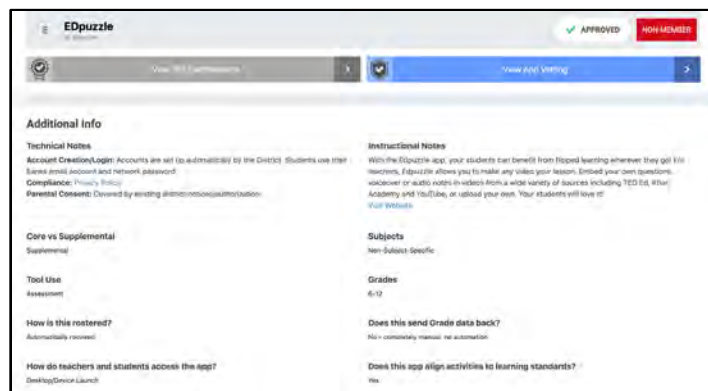
Since the inception of the district's 1:1 program, the district relied on district administrators and teachers to identify and select instructional resources that best met the instructional need or learning objective, without fully understanding the possible repercussions or risks for sharing student and staff data. Utilizing the *TrustEd App Dashboard* and evaluation rubric and structure created by IMS Global, the district can confidentially select instructional resources that align with the district's vision for safety and security. Incorporating third-party reviews into the digital resource process provides additional security measures on not only what students are using, but how they access the resource, what, if any, personally identifiable information the vendor may be collecting, and how the resource is provisioned to users.

The IMS Global evaluation process, developed by a group of K-12 security professionals, includes an in-depth scale and security measures including regulatory compliance ([GDPR](#), [FERPA](#), [COPPA](#) and age level) and an overall product score based on security protocols. The evaluation rubric includes categories such as data collection, security, third party data, and advertising. Individual categories of the evaluation rubric have subcategories where each resource is measured and provided an overall rating based on the vendor responses and evidence submitted during the evaluation process. *See appendix M.*

IMS Global is the world-leading non-profit collaborative agency advancing edtech interoperability standards and data privacy measures for K-12 agencies. IMS created a plug-and play-architecture and ecosystem that provides a foundation on which innovative products can be evaluated and rapidly deployed in schools. The IMS vendor certification is a bond of trust and commitment to creating innovative products that work together for the benefit of instructors, students, and institutions.

Partnering with over 70 K-12 districts, IMS provides an academic focused list of products that align with data privacy standards and security principles ensuring a secure learning experience for students. Digital resources are evaluated and certified by a group of security professionals using the IMS privacy criteria as well as the district's data safety standards. One component of the IMS collaboration is a dashboard of resources providing information to the Eanes academic community as it relates to instructional tools available within the district. Based on the need for a more detailed and thorough resource vetting process, the district will utilize the *TrustED App Dashboard* as a reference and in conjunction with the district's current evaluation process.

The *TrustED App Dashboard* will be fully functioning and available to staff during the 2022-23 school year. The image provides an example of the information available within the district's dashboard. To review the Educational Technology materials.



Technology Services:

Technology Services is a team of individuals, with specialized technical abilities, dedicated to providing quality customer service with layered support for the Eanes ISD academic community. Staff members in this department implement and maintain the infrastructure, applications, and processes to support district initiatives and implementations. *See appendix M.*

In addition to classroom audiovisual hardware, Technology Services team members support more than 15,000 devices including windows desktops, PC laptops, Apple iPads, iMacs, and MacBook laptops. These devices are located across nine schools and other administrative locations across the district. Additionally, Technology Services provides maintenance, support, and professional learning on more than 40 customized applications and systems. Resources supported by the district were funded in part by the 2019 Bond election allowing the department to complete infrastructure upgrades and improvements, provide new devices to students as part of our 1:1 implementation and upgrade audiovisual technologies in all K-12 classrooms. Future bond elections will be a priority and requirement for the district to continue maintenance, replacement, and expansion of technology implementations and applications across the district.

The information included in this section of the document highlights a portion of the services provided to the academic community by the department.

Department Services:

Elementary Green iPad: Eanes ISD believes in providing a safe, supportive digital environment that empowers our learning community through the purposeful and intentional application of standards-driven, best instructional practices. In aligning with a safe digital environment, the district implemented a Green iPad at the elementary level (grades K-5). The Green iPad configuration contains instructionally focused apps, evaluated by staff to ensure alignment with curricular objectives, and is used as a tool for instruction. Each mobile app provisioned to the Green iPad, is evaluated for alignment with the district's guidelines for student data, privacy and security and academic relevance. Additionally, the district maintains multiple filtering processes and enables only websites and internet categories that have been thoroughly vetted and approved for academic purposes. The district continues to evaluate digital resources, including websites and mobile apps to support academic needs, safeguard student privacy and identify best instructional practices.

Web Filters: Eanes ISD takes extensive measures to protect students and staff from accessing inappropriate or malicious web content. Those safety measures include the creation of the restricted iPad, known as the Green iPad for elementary students and the implementation and management of multiple web filters on devices used by all K-12 students. Students, at any level, are given access to filtered web content provisioned with age appropriate restrictions.

In regards to filtering the internet, the district follows the guidelines and requirements for content that is accessible by students on district devices and networks, as well as student data privacy requirements. Adhering to the [Children's Internet Protection Act](#) (CIPA), the [Children's Online Privacy Protection Rule](#) (COPPA) and the [Family Educational Rights and Privacy Act](#) (FERPA), the district currently utilizes three different web filters to restrict inappropriate and malicious content from students and staff.


- The governing web filter for incoming and outgoing web material is Fortinet. Fortinet is designed to block inappropriate content using a category hierarchy prioritization framework that prohibits the end user from accessing websites and inappropriate material.
- The second web filter is Lightspeed. Lightspeed is installed on all mobile devices (iPads) and blocks inappropriate content following a specific category framework, regardless of location. Within Lightspeed, district administrators can override or allow individual websites as needed for classroom instruction. This web filter governs and controls the elementary Green iPad.
- The third web filter resides within the mobile device management system (MDM) JAMF. Profiles and policies within JAMF are applied to individual user groups (grade level specific) and include device specific restrictions such as the inability for students to delete apps on the iPads or to download non-approved mobile apps.

The district continually monitors web filter categories and settings for potential adjustments and areas of improvement.

Gaggle: Eanes ISD maintains a technology application to proactively protect students and ensure their safety and well-being in digital spaces. The district launched the [Gaggle Safety Management](#) solution to monitor student safety on school-provided technology and further promote student and educator productivity in a safe and controlled environment. Eanes ISD utilizes Gaggle to analyze student emails and cloud based applications for inappropriate behavior as well as identify potential serious situations such as self-harm, cyberbullying, substance abuse, threats and more.

Through the district's partnership with Gaggle, administrative staff are informed of potential risks and can respond, intervene or assist students as needed. Relying on Gaggle notifications, campus and district staff can work with families to ensure students are safe from harm.

iPad Protection Plan (EanesCare): Eanes ISD provides the opportunity for students and families to purchase insurance on the devices (iPads) assigned to students. [EanesCare](#) is available for purchase annually and provides coverage for possible damage, theft or loss of individual student devices. This iPad protection plan provides coverage to families for a minimal cost and is used only in the event a student device is in need of repair or replacement.

| |  Purchase of the EanesCare Protection Plan is Optional. | <div>EANESCARE</div> <div>\$ 25</div> | <div>NO PROTECTION PLAN</div> <div>Decline EanesCare</div> <div>\$ 0</div> |
|----------------------------------|---|--|---|
| | | | |
| Coverage | | Includes EanesCare Protection Coverage for Accidental Damage, Loss or Theft of iPad and case. | You are Responsible for Full Cost of the Replacement of iPad & All Accessories for Loss, Theft, and Damages |
| Claims | | Maximum of 2 Claims Per School Year Additional Claims Subject to Full Replacement or Repair Costs | — |
| Accidental Damage Claim Coverage | | \$0 Deductible Per Incident Maximum of 2 Incidents Per School Year Covered Includes broken screen, broken charging port, dented casing, etc. Does Not Cover Vandalism | Approximately \$523 to Replace Damaged iPad and Case |
| Loss Claim Coverage | | EanesCare will pay 50% of replacement cost. Plan holder is responsible for 50% of replacement cost. Approx. plan holder cost: iPad and case \$261.50 | Approximately \$523 to Replace Lost iPad and Case |
| Theft Claim Coverage | | EanesCare will pay 70% of replacement cost. Plan holder is responsible for 30% of replacement cost. Claim requires police report. Approx. plan holder cost: iPad and case \$156.90 | Approximately \$523 to Replace Stolen iPad and Case |
| Coverage Dates | | September 1 - August 31 Coverage is for one school year | — |

*All costs are estimates and are subject to change without notice.

Each year the district has approximately 5-10% damage or repairs on student and staff devices. The funds generated by the EanesCare protection plan covers the costs of all repairs or replacements.

Data Integrations and Rostering: The Technology Services department is responsible for all data integrations, syncing student and staff information between resources, and student account rostering within software applications and digital textbooks. Following security protocols, staff members create, maintain and implement data synchronization between the student information system, Skyward, and other applications.

Data integrations and synchronizations are automated and completed each evening. Student and staff data are retained within the appropriate applications and are regularly backed up using a variety of methods. Technology staff monitor status of all synchronizations and audit reports to ensure data integrations are secured and reflect accurate data.

Textbook Adoptions: In partnership with the district's Curriculum and Instruction department, Technology Services provides input into the selection and adoption of all digital textbooks to ensure technical requirements and specifications of the product aligns with the district's rostering and data integration protocols. During the textbook adoption cycle, content committee members, including a representative of the Technology Services department, evaluate instructional materials using the following technical specifications (list does not include instructional requirements):

- Is the textbook compatible with iOS devices (iPads)?
- Do the instructional materials include interactive resources, assessments, images or graphs?
- Is the textbook available regardless of browser (Chrome, Safari, etc.)?
- What rostering applications are compatible with the instructional materials (Clever, Rapid Identity, etc.)?
- Does the application require third-party resources (ExamView, PDF reader, etc.)?
- How do students gain access to the instructional materials (SSO, Google, etc.)?

District Infrastructure:

To provide a secured and reliable learning experience for all users, Technology Services must provide and maintain a robust, state of the art infrastructure, with applications and systems that align with the district's expectations for technology. As part of the infrastructure requirements, Technology Services partners with the district's Maintenance and Operations department to provide and support a variety of safety and security measures including security monitoring systems, keyless entry, visitor and volunteer management systems, and secured entry badging access for staff members. The infrastructure items included in this technology plan are the primary responsibility of staff members of Technology Services.

Applications: Students and staff utilize a variety of applications and systems to complete and or manage tasks either because of their position or as part of the learning process. Most of the essential systems and applications are hosted by vendors and stored virtually. Any outages, service interruptions or upgrades are completed by the hosting vendor in partnership with Technology Services staff members. In the event of a district outage (electrical, internet or other), the cloud-based solutions would still be accessible to students and staff.

The district currently maintains a few systems on-premise. Those systems (on-premise) are located at the District's network operations center (NOC) and are contained within the secured, climate-controlled server room. In the event of an outage, service interruption or upgrade, department staff members are responsible for completing the required maintenance on each of the in-house applications and restoring access to users.

Eanes ISD System and Applications:

The table below includes a list of essential applications supported and maintained by Technology Services. Each system provides staff with specific functions, workflows and access to support district operations.

| System/Application and Equipment | Hosted or Cloud-based | On-premise | Available remotely |
|---|-----------------------|------------|--------------------|
| Skyward | ✓ | | ✓ |
| Active Directory | | ✓ | |
| Clever | ✓ | | ✓ |
| ID Auto | ✓ | | ✓ |
| JAMF | ✓ | | ✓ |
| Google Apps | ✓ | | ✓ |
| Google Mail | ✓ | | ✓ |
| Eduphoria | ✓ | | ✓ |
| Kaseware | ✓ | | ✓ |
| Mobile Apps | ✓ | | ✓ |
| Instructional Resources | ✓ | | ✓ |
| Library Resources | ✓ | | ✓ |
| Learning Management Systems | ✓ | | ✓ |
| Ricoh Copy Machines | | ✓ | |
| Desk Phones & Voicemail | | ✓ | |
| Physical & Virtual Networks | | ✓ | |

Skyward: Applications included within the student information system include the following components: finance, human resources, employee access, student admin, gradebook, family and student access. Each of these modules would continue to function and be available remotely allowing staff and students to access the content within each module.

Active Directory: Active directory is the application used by the district to create, manage and assign user accounts and security levels. In the event of a power outage, this server would not be available on site but would be accessible remotely by Technology Services staff. The AD server syncs data to Clever, Skyward and ID Auto and would not continue to send data to those cloud-based solutions until power was restored to the district.

Clever & ID Auto: The district utilizes two different rostering applications - Clever and ID Auto ([textbook portal](#)). Both systems are hosted in the cloud but are synced to active directory (AD) which is hosted on-premise. In the event of an outage, Clever and ID Auto would be available remotely but would not be able to sync any updates until the AD server was back online and sending the updated information.

JAMF: JAMF is the application used by the district to manage all Apple iPads and MacBooks. This system is hosted by the vendor and would be available remotely. The limitation of JAMF is that it relies on devices having internet connectivity to apply changes. The devices, with charged batteries, would continue to function with JAMF offline, but would not receive any updates from the system until the device connects to a wired or wireless network.

Google Apps & Email: The district uses Google applications for productivity, scheduling and email. The Eanes domain is hosted on Google servers and would be available for students and staff remotely. Communications sent during the power outage would be received by the users using a battery powered device or when the electrical issue has been resolved.

Eduphoria: Eduphoria is another application that is hosted in the cloud and would be accessible to staff members remotely. Eduphoria contains a variety of district systems including Helpdesk, professional development catalog and teacher appraisal system. The application is synced with the Active Directory (AD) server and would therefore not be updated until the AD server was back online and sending updated data to Eduphoria.

Kaseware: Kaseware is the case management application used by the district to document incidents, lost or stolen devices and staff inventory. This application is managed in partnership with the district's Maintenance & Operations department. During a power outage, Kaseware would be accessible remotely.

Mobile Apps & Instructional Resources: The majority of digital resources used in classrooms across the district are hosted by third party vendors. These resources, such as mobile apps and web-based resources, would be available to any user with internet access.

Library Resources: The libraries in Eanes utilize multiple online subscriptions and applications including Follett Destiny, the application that allows users to access digital books and materials. These library resources are hosted by vendors and would be available to students and staff remotely with no change in expected functionality.

Learning Management Systems: The district currently uses three separate systems as learning management systems (LMS). [Google Classroom](#), [Seesaw](#) and [Showbie](#) are all hosted by vendors and would continue to be accessible by students and staff remotely.

Ricoh Copy Machines: The Ricoh copy machines, located in each building across the district, would not be accessible to staff during a power outage. Once the power was restored the machines would be accessible onsite.

Desk Phones and Voicemails: The district currently using phones, voice over IP (VOIP) are all reliant on electricity and would not be available to staff without power.
**All landlines would remain functioning and available in case of an emergency.*

Physical & Virtual Networks: The district's network consists of a variety of devices including servers, switches, routers and wireless access points. Depending on the location of the incident, the physical hardware may or may not be impacted. Technology Services staff partners with vendors to manage each piece of equipment and would be responsible for restoring access to users.

Retirement Considerations:

When removing technology hardware from classrooms, campuses, or district buildings, typically when the equipment is end of life or is no longer supported by the manufacturer, the district must follow local and federal standards for recycling, secure destruction, or resale. Any end of life technology items, originally purchased using district bond funds the district is required to follow guidelines placed on us by the legal parameters surrounding the use of bond funds (taxpayer dollars). For devices removed from inventory, and originally funded using bond dollars, the district must follow bond regulations requiring the devices be sold using an approved third-party vendor. Devices that are still in working condition and have residual value must be sold at fair market value with any funds gained through the sale of the devices placed back into district budgets for future purchase of technologies.

Guiding Principles:

The principles, goals and priorities of the Eanes ISD technology plan are aligned with the annual goals and priorities set forth by the Board of Trustees. The goals within the technology plan, and created with input from the Technology Advisory Committee, will be reviewed and updated as new goals and priorities are identified by the Board of Trustees. Guiding principles for Technology Services are listed below. These statements are foundational to the work and support efforts of the department.

- Academic technology products, services and projects will be evaluated and supported to benefit the Eanes ISD educational goals and board priorities.
- A focus will be maintained on supporting the core mission of *Thoughtful Use of Technology* while identifying new solutions and technology applications.
- Students and staff will have well-supported, secure, and reliable access to information and technology resources.
- Assistive technologies will be provided as appropriate to ensure access to educational programming and content for all students.
- Professional development is the foundation of successful technology integration.
- Technology initiatives will be leveraged to accelerate the integration of educational technology into instructional practice and classroom instruction.
- Technology initiatives will be enhanced by the unique skills and abilities that our students and staff bring to the learning environment.
- Customer service is the utmost priority and the responsibility of each member of the department.

Goals and Objectives:

Following the charge to the Technology Advisory Committee, the members have identified the following goals for the district's Technology Services and Educational Technology teams to guide the work, initiatives and implementations for upcoming school years. These goals, and progress towards the goals, will be monitored annually by the Technology Advisory Committee and district administrators to ensure the alignment with district, Board, and department priorities and initiatives.

The goals of this plan align with the district's current priorities and guiding principles for Technology Services. Additional goals were identified to further the progress of technology integration across the district. The [2021-22 board priorities](#) for the department are listed below:

- **Maintain a long-range plan for operational processes.**
- **Safeguard students, staff and resources by securing schools and cyber technologies.**
- **Examine and re-evaluate budget priorities in preparation for or in response to evolving circumstances.**

The goals, objectives and tasks of this technology plan are included on the next pages. Each goal is measurable and contain multiple tasks for completion towards progress.

Eanes ISD Instructional Priority: A Culture of Guaranteed Viable Curricula (GVC)

Goal 1: Using an evaluation matrix, the district will identify exemplary learning management systems (LMS) as a possible K-12 solution by the 2023-24 school year.

| | |
|---|--|
| Objective 1: Create an evaluation matrix incorporating non-negotiables from stakeholder groups. | <i>Task 1.a)</i> Conduct stakeholder meetings to identify non-negotiables from community, students, staff, administrators, and other user groups. |
| | <i>Task 1.b)</i> Develop final list of non-negotiables from stakeholder interviews. |
| | <i>Task 1.c)</i> Create matrix for conducting evaluations of learning management systems. |
| Objective 2: Identifying LMS solutions that best align with the district's needs. | <i>Task 2.a)</i> Using a feature comparison chart, select the system that best meets the needs of the entire academic community including professional development opportunities and ongoing support for all stakeholder groups. |
| | <i>Task 2.b)</i> Identify 2-3 systems that best align with the stakeholder's needs. |
| | <i>Task 2.c)</i> Conduct vendor demonstrations and evaluations with stakeholders for input into the final selection process. |
| Objective 3: Relying on the identified non-negotiables, feature comparison and stakeholder feedback, make LMS recommendations. | <i>Task 3.a)</i> Complete purchase processes, vendor contract and service agreements. |
| | <i>Task 3.b)</i> Begin project management meetings with the vendor to identify customizations, integrations and technical specifications for full implementation. |
| | <i>Task 3.c)</i> Develop communication plan and informational website for project. |
| | <i>Task 3.d)</i> Create a professional development calendar, training model and support resources for all stakeholder groups. |
| | <i>Task 3.e)</i> Complete integrations and implementation of the system including archiving previous systems. |
| | <i>Task 3.f)</i> Begin professional development and plan for multi-staged implementation with stakeholder groups. |

Eanes ISD Operational Priority: Operations and Long-Range Planning

Goal 2: Identifying future funding opportunities, the district will maintain state of the art infrastructure and end user technologies representative of the ever evolving needs of learners by focusing on a 4-year refresh cycle.

| | |
|--|---|
| Objective 1: Review and evaluate technologies based on academic need, solution and application. | <i>Task 1.a)</i> Identify infrastructure requirements to support new district initiatives. |
| | <i>Task 1.b)</i> Adopt a refresh cycle for hardware and infrastructure equipment. |
| Objective 2: Identify funding opportunities to purchase and maintain technologies and infrastructure. | <i>Task 2.a)</i> Following the recommendations of the Board of Trustees, develop hardware and software requirements for future bond elections. |
| | <i>Task 2.b)</i> Using bond and department funding, create a responsible budgeting and purchasing model that aligns with the district's procurement processes. |
| | <i>Task 2.c)</i> Following current bond oversight procedures and governance, ensure accountability and fiscal management. |
| Objective 3: Evaluate and recommend infrastructure and user technologies. | <i>Task 3.a)</i> Review existing infrastructure service level agreements and contracts to identify resources that are end of life or require upgrades or maintenance. |
| | <i>Task 3.b)</i> Based on academic needs and district goals and priorities, identify technologies that best align with future needs of the district. |
| | <i>Task 3.c)</i> Prior to a refresh cycle of 1:1 devices for students, reconvene focus groups and the Technology Advisory Committee to obtain feedback and input into the device selection and recommendations. |
| | <i>Task 3.d)</i> Conduct a site audit on all audio visual equipment utilized on campuses to determine support needs or replacement plans. |

Eanes ISD Instructional Priority: A Guaranteed and Viable Curricula (GVC)

Goal 3: Prioritizing the district's beliefs regarding the *Thoughtful Use of Technology*, the district will provide learning opportunities for staff by offering professional development, emphasizing universal design for learning (UDL) and technology integration (SAMR) concepts, in alignment with new district implementations.

| | |
|--|---|
| Objective 1: Identify professional development topics and timeline. | <i>Task 1.a)</i> Create and maintain a calendar of professional development opportunities for all staff. |
| | <i>Task 1.b)</i> Develop just in time professional development topics for all stakeholder groups based on project or technology initiative. |
| | <i>Task 1.c)</i> Develop and maintain professional development resources for all stakeholder groups. |
| Objective 2: Select district employees to develop and lead professional development and create resources. | <i>Task 2.a)</i> Develop a professional development support model and delivery platform (train the trainers, face-to-face, online, etc.) for all users. |
| | <i>Task 2.b)</i> Provide targeted professional development at all campuses, emphasizing thoughtful use and best instructional practices. |
| Objective 3: Provide and maintain ongoing support for instructional staff and students. | <i>Task 3.a)</i> Relying on the Educational Technology team, create and maintain a variety of multi-leveled resources and support plans for all district initiatives. |
| | <i>Task 3.b)</i> Promote continued professional development opportunities, varied in level and delivery model, accessible to all staff members. |
| | <i>Task 3.c)</i> Evaluate and revise professional development resources as needed for continued support of the academic community. |

Eanes ISD Operational Priority: Operations Long-Range Planning

Goal 4: To ensure the safety of students and staff, the district will prioritize cybersecurity and opportunities.

| | |
|--|---|
| Objective 1: Notify users of potential security risks and provide best practices involving the use of personal devices and district issued accounts connected to district networks. | <i>Task 1.a)</i> Generate reports, review data and complete safety notifications to identified users. |
| | <i>Task 1.b)</i> Provide professional development opportunities for using data privacy strategies to identify and review appropriate instructional resources. |
| | <i>Task 1.c)</i> Maintain, create and share a variety of safety protocols and best practices with students and staff. |
| Objective 2: Implement and maintain additional safety and risk management measures on district systems and applications. | <i>Task 2.a)</i> Identify and implement cybersecurity measures on all district resources, systems and technologies to provide additional safety layers for users. |
| | <i>Task 2.b)</i> Educate and promote safety measures and risk management practices with district users. |
| | <i>Task 2.c)</i> Update and maintain a cybersecurity plan inclusive of safety protocols and risk management options. |
| Objective 3: Develop and maintain department governance manual, inclusive of systems preparedness and incident response procedures. | <i>Task 1.a)</i> Create and update documentation of security protocols for each system and application used within the district. |
| | <i>Task 1.b)</i> Update and maintain service level agreements and documentation for all vendors and manufacturers of infrastructure hardware and software. |
| | <i>Task 1.c)</i> Conduct audits and assessments on infrastructure, data center and phone systems to verify vulnerabilities and potential risks. |
| | <i>Task 1.d)</i> Complete maintenance and remediation steps, identified by audits, to ensure a reliable and safe environment for all district users. |
| | <i>Task 1.e)</i> Keep technologies at maximum performance levels, complete maintenance and required technical upgrades on existing infrastructure. |

Eanes ISD Operational Priority: Operations and Long-Range Planning

Goal 5: The district will continue to emphasize *Thoughtful Use of Technology*, by evaluating applications and digital resources (mobile apps, YouTube, etc.) incorporated into classroom instruction and accessed by students for academic relevance, appropriateness, and integration.

| | |
|---|---|
| Objective 1: Partner with classroom teachers and campus administrators, to identify and evaluate digital resources and applications used by grade level. | <i>Task 1.a)</i> Review and revise as needed, the district's vision and definition for <i>Thoughtful Use of Technology</i> . |
| | <i>Task 1.b)</i> Generate inventory of applications and digital resources used by level (elementary, middle and high school). |
| | <i>Task 1.c)</i> Re-evaluate the terms of service and privacy policy of items included on digital resource inventory. |
| | <i>Task 1.e)</i> As needed, identify alternate resources for applications that no longer align with the district's vision for technology integration and thoughtful use. |
| Objective 2: Reconvene teacher focus groups to review instructional practices and digital resources to support classroom management and foster self-regulation for students. | <i>Task 1.a)</i> Identify leveled focus group (K-12) members with representation from each campus. |
| | <i>Task 1.b)</i> Develop objectives and timeline for each group, emphasizing classroom management and self-regulation for students. |
| | <i>Task 1.c)</i> Create an inventory of digital resources, available by level, including funding source, classroom application and rostering process. |
| | <i>Task 1.d)</i> Update evaluation rubrics to reflect K-12 restrictions, specifications and requirements. |
| | <i>Task 1.e)</i> Partner with campus Educational Partners, Educational Technologists, Administrators and the Curriculum and Instruction team to refine the inventory of digital resources and identify potential funding opportunities for newly selected applications. |
| | <i>Task 1.f)</i> Following district purchasing processes, obtain new resources and complete integrations with the Technology Services team. |
| | <i>Task 1.g)</i> Create tutorials and conduct professional development for all K-12 staff impacted by new initiatives. |

Future Planning & Vision:

In alignment with the goals of this plan, and elements identified on the [District's Improvement Plan](#), both Technology Services and Educational Technology teams have identified additional initiatives to further expand services offered to the academic community.

Relying on the foundation of this technology plan and the District's improvement plan, Technology Services will research and identify additional elements, applications and services that best meet the evolving needs of the students and staff of Eanes ISD. Future planning and visioning for the department is ongoing but this technology plan will provide evidence and rationale for future technology initiatives.

Future Initiatives:

Security Measures: The district will identify and implement additional security measures as it relates to protecting student and staff data. One new initiative could include adding data encryption software to district staff email accounts allowing information to be shared only with the intended recipients, preventing data from being accessed by non-authorized users. Adding encryption software to staff email accounts places another layer of governance, safety, and risk management on all content and attachments containing personally identifiable information (PII).

CyberSecurity: The department will need to emphasize the security and risk management strategies, applied to all applications, including appropriate security levels, district impact, response plan and develop a tiered support model.

Asset Management: To further expand the department's inventory processes, the district will implement an inventory management system that transforms current department asset management applications and allows advanced reporting, tracking and replacements. The inventory management system would integrate into existing systems and streamline department processes and procedures.

Department Governance: The department will create, compile and maintain a manual documenting all department processes and workflows for change management, editing user accounts, vendor management and security protocols. The documentation will be updated annually or as new resources are added to the infrastructure.

Video Streaming Solution: As part of the instructional priorities, the department will need to identify video streaming solutions that align with copyright and best instructional practices. The solution will need to be vetted by instructional staff and reviewed for level, quantity and quality of content across all curriculum areas.

Remote Desktop Management: In an attempt to provide an advanced level of customer service, the department will investigate a remote desktop management system (helpdesk) allowing Technology Services team members to remote into user devices to identify issues and resolve problems without having to travel to campuses, extend response time or postpone resolution for users.

Professional Development: The District believes that professional development and training are priorities and a requirement for all successful implementations. The department will prioritize and emphasize professional development opportunities for all support staff interacting with any new technology hardware, application or system. Providing support and training for department staff will continue to be a priority and goal for the department.

Conclusion:

Moving forward, the Technology Advisory Committee charges the district to implement, support and maintain products and resources that align with the goals presented in this technology plan. These goals, and progress towards the goals, should be evaluated by district administrators and the Technology Advisory Committee. As circumstances and technologies change, any necessary revisions or additions can be embedded into this technology plan. TAC members will continue to provide input, guidance and support for all district technology initiatives.

Using the sample table format below, progress towards the goals and objectives outlined in this plan will be assessed. Progress, evidence and evaluation measures will be documented and added as an addendum to this technology plan.

| | | |
|----------------------------|----------------------------|-----------------|
| Eanes ISD Priority: | | |
| Goal: | | |
| Objective: | | |
| Tasks | Implementation Team | Evidence |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

References:

- CAST (2018). Universal Design for Learning Guidelines version 2.2. Retrieved from <http://udlguidelines.cast.org>
- European Commission: General Data Protection Regulation (GDPR), 2022. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection_en
- Federal Communications Commission: Children's Internet Protection Act (CIPA), 2022. Retrieved from <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>
- Federal Trade Commission: Children's Online Privacy Protection Rule (COPPA), 2022. Retrieved from <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>.
- Gaggie (2022). Retrieved from <https://www.gaggie.net/>.
- IMS Global Consortium (2022). Retrieved from <https://www.gaggie.net/>.
- ISTE Standards for Students, ©2022, ISTE (International Society for Technology Standards in Education). *ISTE*. Retrieved from <https://www.iste.org/>.
- Texas Education Agency (TEA), Building a Strong Texas: Long-Range Plan for Public Education (2018-2023). Retrieved from <https://tea.texas.gov/sites/default/files/Long-Range-Technology-Plan.pdf>.
- Texas Essential Knowledge and Skills (TEKS), 19 TAC Chapter 126. Retrieved from <https://tea.texas.gov/academics/curriculum-standards/teks-review/technology-applications-teks>.
- U.S. Department of Education: Family Educational Rights and Privacy Act (FERPA), 2022. Retrieved from <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

Appendices

Technology Resources

Eanes ISD Policy CQ

The district's technology resources, including its networks, computer systems, email accounts, devices connected to its networks, and all district-owned devices used on or off school property, are primarily for administrative and instructional purposes. Limited personal use is permitted if the use:

- Imposes no tangible cost to the district
- Does not unduly burden the district's technology resources
- Has no adverse effect on job performance or on a student's academic performance

Electronic mail transmissions and other use of technology resources are not confidential and can be monitored at any time to ensure appropriate use.

Employees are required to abide by the provisions of the district's acceptable use procedures. Failure to do so can result in suspension of access or termination of privileges and may lead to disciplinary action and legal action. Employees with questions about computer use and data management can contact the Director of Technology Services, at extension 20703.

The District's Responsible Use Guidelines for Technology can be found at the end of this Handbook and on the employee Intranet.

Professional Use of Electronic Communications

Eanes ISD Policy CQ, DH, Responsible Use Guidelines

Eanes Independent School District recognizes the importance of faculty, students and parents engaging, collaborating, learning and sharing in the digital environments as part of 21st century learning. The professional use of electronic media (as defined below in *Personal Use of Electronic Media*), is encouraged as a vehicle to further the educational and administrative purposes, goals, and objectives of the district. Accordingly, such use must be appropriate, not disruptive to the educational environment, and not detrimental to personal interactions with students and parents.

The District requires the use of a managed Apple ID and Google accounts for District work done on District-owned devices. Personal accounts and user IDs should not be used on District-owned devices or for District work. An employee utilizing or merging personal Apple IDs and cloud-based services with their managed Apple ID or Google account on District-owned devices risks intermingling their personal and professional information.

Eanes ISD implemented a new technology application to proactively protect students and ensure their safety and wellbeing in digital spaces. The district launched Gaggle Safety Management solution to manage student safety on school-provided technology and further promote student and educator productivity in a safe and controlled environment. Eanes ISD utilizes Gaggle to have the ability to analyze emails between student and staff for inappropriate behavior as well as identify potential serious situations such as self-harm, cyberbullying, substance abuse, threats and more. Employees using electronic media for professional purposes shall comply with the terms and conditions established in the district's Responsible Use Guidelines.

Personal Use of Electronic Communications

Eanes ISD Policy CQ, DH, Acceptable Use Guidelines

Electronic communications includes all forms of social media, such as text messaging, instant messaging, electronic mail (email), web logs (blogs), wikis, electronic forums (chat rooms), video-sharing websites (e.g., YouTube), editorial comments posted on the Internet and social network sites (e.g., Facebook, Twitter, LinkedIn, Instagram). Electronic communications also includes all forms of telecommunication such as landlines, cell phones, and web-based applications.

As role models for the district's students, employees are responsible for their public conduct even when they are not acting as district employees. Employees will be held to the same professional standards in their public use of electronic communications as they are for any other public conduct. If an employee's use of electronic communications interferes with the employee's ability to effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment. If an employee wishes to use a social network site or similar media for personal purposes, the employee is responsible for the content on the employee's page, including content added by the employee, the employee's friends, or members of the public who can access the employee's page, and for Web links on the employee's page. The employee is also responsible for maintaining privacy settings appropriate to the content.

An employee who uses electronic communications for personal purposes shall observe the following:

- The employee may not set up or update the employee's personal social network page(s) using the district's computers, network, or equipment.
- The employee shall limit use of personal electronic communication devices to send or receive calls, text messages, pictures, and videos to breaks, meal times, and before and after scheduled work hours, unless there is an emergency or the use is authorized by a supervisor to conduct district business.
- The employee shall not use the district's logo or other copyrighted material of the district without express, written consent.
- An employee may not share or post, in any format, information, videos or pictures obtained while on duty or on district business unless the employee first obtains written approval from the employee's immediate supervisor. Employees should be cognizant that they have access to information and images that, if transmitted to the public, could violate privacy concerns.
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Texas Educator's Code of Ethics, even when communicating regarding personal and private matters, regardless of whether the employee is using private or public equipment, on or off campus.

These restrictions include:

- Confidentiality of student records [See Policy FL]
- Confidentiality of health or personnel information concerning a colleague, unless disclosure serves lawful professional purposes or is required by law. [See DH (EXHIBIT)]
- Confidentiality of district records, including educator evaluations and private email addresses. [See Policy GBA]
- Copyright law [See Policy CY]
- Prohibition against harming others by knowingly making false statements about a colleague or the school system [See DH(EXHIBIT)]

See Electronic Communications between Employees, Students, and Parents, below, for regulations on employee communication with students through electronic media.

Appendix D: Responsible Use Guidelines (Staff):

Eanes Independent School District Staff Responsible Use Guidelines for Technology

Technology is essential to facilitate the creative problem-solving, information fluency, communication and collaboration that we see in today's global economy. The Responsible Use Guidelines (RUG) support our vision of responsible technology use and promote a strong sense of digital citizenship. The RUG applies to all Eanes Independent School District computer networks (including the devices made available by them), and all devices connected to those networks (whether they be staff-owned or otherwise).

With the ability to use technology comes responsibility. It is important that you read and discuss the District Responsible Use Guidelines, ask questions if you need help in understanding them, and sign the agreement form. It will be your responsibility to follow the rules for appropriate use. Irresponsible system use will result in the loss of the privilege of using this educational and administrative tool.

Please note that the Internet is a network of many types of communication and information networks. It is possible that you may run across some material you might find objectionable. While Eanes ISD will use filtering technology to restrict access to such material, it is not possible to absolutely prevent such access.

Please note that the Internet is a global computer network of many types of communication and information networks. It is possible that users may run across some material that might be considered objectionable. While Eanes ISD will use Internet filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. District provided resources are not private and may be viewed by district officials. The school district will provide use of third party accounts (such as Google Apps) that must also adhere to these Responsible Use Guidelines. Any other third party accounts that are used for educational purposes, must also adhere to these Responsible Use Guidelines. Eanes Independent School District will monitor user activity on the network and on school-issued devices.

The District requires the use of a managed Apple IDs and Google accounts for District work done on District-owned devices. Personal accounts and user IDs should not be used on District-owned devices or for District work. An employee utilizing or merging personal Apple IDs and cloud-based services with their district managed Apple ID or Google account on District-owned devices are at risk of intermingling their personal and professional information.

Eanes ISD provides access to District technology assets for work-related activities. Use of District technology assets should be in accordance with applicable District policies, administrative regulations, and the guidelines set herein. Inappropriate use of technology assets may result in loss of privileges, as well as other disciplinary or legal action. In consideration for the District permitting use of the equipment for personal business, the employee assumes financial responsibility for negligent damage of the equipment. Eanes ISD may issue the employee district-owned assets. This equipment is authorized for the employee's use until the employee is no longer employed by the District or the employee fails to comply with the Responsible Use Guidelines, or District policy. Employees are responsible for turning in all technology to Eanes ISD Technology Services prior to the last day of employment unless otherwise directed by the Superintendent or designee.

It will be your responsibility to follow the rules for appropriate use.

RESPONSIBLE USE AND DIGITAL CITIZENSHIP

Any use described below is deemed “responsible” and consistent with the Eanes ISD Responsible Use Guidelines for Technology. The final decision regarding whether any given use of the network or Internet is acceptable lies with the Superintendent or designee.

- Use is mainly for educational purposes, but some limited personal use is permitted. (Remember that people who receive email from you with a District address might mistakenly infer that your message represents the District’s point of view).
- Use furthers the educational and administrative purposes, goals, and objectives of Eanes ISD.
- Use is limited to your own individual account - you and only you should use that account. You should not share your password with others.
- Use furthers research related to education and instruction
- Use does not violate employee standards of conduct.
- Use of appropriate online names as well as use of polite and appropriate language/content on all online posts.
- Use of websites, content, and media is properly cited with respect to copyright.

UNACCEPTABLE AND IRRESPONSIBLE USE

Any of the following uses is deemed “unacceptable and irresponsible” and a violation of the Eanes ISD Responsible Use Guidelines for Technology. This list does not include all possible violations. The final decision regarding whether any given use of the network or Internet is acceptable lies with the Superintendent or designee.

Disciplinary action may be taken for unacceptable and irresponsible use of the network or Internet.

- Unauthorized use of copyrighted material, including violating district software licensing agreements
- Sending or posting messages and/or content that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another’s reputation, illegal, or intended to bully
- Use of technology resources such as chat rooms, social sites, and games in a manner that causes disruption to the educational program
- Posting videos of photos of staff or students online without permission.
- Use of school technology resources to encourage illegal behavior or threaten school safety
- Use of social media, messages, private cloud storage and/or email, on or off campus, personal or otherwise, in violation of the Code of Ethics and Standard Practices for Texas Educators which include any violation of the following; confidentiality of student records, health or personnel information concerning colleagues, district records (including evaluations and private email addresses), copyright law, illegal activities, harming others by knowingly making false statements about a colleague or the school system.
- Personal, political use to advocate for or against a candidate, office-holder, political party, or political position. Research or electronic communications regarding political issues or candidates shall not be a violation when the activity is to fulfill an assignment for class credit.
- Use of any means to disable or bypass the district’s Internet filtering system or other security systems

- Use of personal device that conflicts with Board policy and/or the employee handbook
- Attempting to alter, destroy, disable or gain unauthorized access to district technology equipment, district data, the data of other users, or district network resources.
- Damage or loss of district-issued technology equipment via negligence or purposeful actions.
- Encrypting communications or files to avoid security review
- Posting personal information about yourself or others (such as addresses and phone numbers) other than as needed to conduct school operations
- Forgery of electronic mail messages or transmission of unsolicited junk email
- Use related to commercial activities or for commercial gain
- Use that violates employee standards of conduct, or is unlawful
- Wasting school resources through the improper use of the computer and/or network systems

One or more of the following consequences may be imposed:

- Suspension of access to the system
- Revocation of the computer system account
- Removal of device access
- Other action, including disciplinary action, in accordance with Board policy and/or the Employee Standards of Conduct.

CONSEQUENCES FOR INAPPROPRIATE USE

Employees should review the Employee Handbook for specific guidelines and prohibitions with regard to communicating electronically with students.

ELECTRONIC COMMUNICATIONS WITH STUDENTS

Eanes ISD implemented a new technology application to proactively protect students and ensure their safety and well-being in digital spaces. The district launched the Gaggle Safety Management solution to manage student safety on school-provided technology and further promote student and educator productivity in a safe and controlled environment.

Eanes ISD utilizes Gaggle to have the ability to analyze emails between student and staff for inappropriate behavior as well as identify potential serious situations such as self-harm, cyberbullying, substance abuse, threats and more.

Appendix E: Responsible Use Guidelines (Elementary Students):

Eanes Independent School District Elementary School Responsible Use Guidelines for Technology

Our staff and students use technology to learn. Technology is essential to facilitate the creative problem-solving, information fluency, communication and collaboration that we see in today's global economy. While we want our students to be active contributors in our connected world, we also want them to be safe, legal, and responsible. The Responsible Use Guidelines (RUG) support our vision of responsible technology use and promote a strong sense of digital citizenship. The RUG applies to all Eanes Independent School District computer networks, digital resources, and all devices connected to those networks (whether they be student owned or otherwise).

With the ability to use technology comes responsibility. It is important you read and discuss the District Responsible Use Guidelines, ask questions if you need help understanding them, and sign the agreement form. It is your responsibility to follow the rules for appropriate use. Irresponsible system use will result in the loss of the privilege of using this educational and administrative tool. Please review the leveled-guidelines following this document, which explain in greater detail responsible use expectations for elementary, middle school and high school students in the areas of Internet Safety & Security, Digital Citizenship, and Research & Information Literacy.

Please note that the Internet is a global computer network of many types of communication and information networks. It is possible that you may run across some material you might find objectionable. While Eanes ISD will use Internet filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. District provided resources are not private and may be viewed by district officials. The school district will provide you with third party accounts (such as Google Apps) that must also adhere to these Responsible Use Guidelines. Any other third party accounts that are used for educational purposes, must also adhere to these Responsible Use Guidelines. Eanes Independent School District will monitor your activity on the network and on school-issued devices.

It will be your responsibility to follow the rules for appropriate use.

RESPONSIBLE USE AND DIGITAL CITIZENSHIP

Any use described below is deemed "responsible" and consistent with the Eanes ISD Responsible Use Guidelines for Technology. The final decision regarding whether any given use of the network or technology resource is acceptable lies with the Superintendent or designee.

- Use is mainly for educational purposes, but some limited personal use is permitted. (Remember that people who receive Email from you with a District address might mistakenly infer that your message represents the District's point of view).
- Use furthers the educational and administrative purposes, goals, and objectives of Eanes ISD.
- Use is limited to your own individual account - you and only you should use that account. You should not share your password with others.
- Use furthers research related to education and instruction
- Use does not violate the student code of conduct or employee standards of conduct.
- Use of appropriate online names as well as use of polite and appropriate language/content on all online posts.
- Use of websites, content, and media is properly cited with respect to copyright.

UNACCEPTABLE AND IRRESPONSIBLE USE

Any of the following uses is deemed “unacceptable and irresponsible” and a violation of the Eanes ISD Responsible Use Guidelines for Technology. This list does not include all possible violations, and supplements prohibited behaviors defined in the Student Code of Conduct. The final decision regarding whether any given use of the network or technology resource is acceptable lies with the Superintendent or designee.

Disciplinary action may be taken for unacceptable and irresponsible use of the network or Internet.

- Unauthorized use of copyrighted material, including violating district software licensing agreements
- Posting of videos or photos without permission of the individual or group.
- Sending, possessing, delivering, or posting electronic messages or images that are abusive, obscene, sexually oriented, harassing, threatening, intimidating, illegal, or that cause a material or substantial disruption at school or infringes on the rights of another student at school, including cyberbullying.
- Use of technology resources such as chat rooms, social sites, and games in a manner that causes disruption to the educational program
- Use of school technology resources to encourage illegal behavior or threaten school safety
- Use of personal device that conflicts with Board policy and/or the student handbook and code of conduct
- Use of any means to disable or bypass the district’s Internet filtering system or other security systems.
- Attempting to alter, destroy, disable or gain unauthorized access to district technology equipment, district data, the data of other users, or district network resources.
- Encrypting communications or files to avoid security review
- Posting personal information about yourself or others (such as addresses and phone numbers) other than as needed to conduct school operations
- Forgery of email messages or transmission of unsolicited junk email
- Use related to commercial activities or for commercial gain
- Use that violates the student code of conduct or employee standards of conduct, or is unlawful
- Wasting school resources through the improper use of the computer and/or network systems

One or more of the following consequences may be imposed:

- Disciplinary action, in accordance with Board policy and/or the student handbook and code of conduct (as applicable)
- Removal of personal device(s) if applicable by authorized District personnel

CONSEQUENCES FOR INAPPROPRIATE USE

Internet Safety and Security

Go Places Safely and Responsibly - The internet can be a great place to discover and visit far-away places to learn new things. Staying safe online is similar to staying safe in the world. Students will choose safe, age-appropriate sites with the guidance of their teachers.

Staying Safe Online - EISD has filters in place to help steer students clear of inappropriate content; however, students may encounter some inappropriate information and/or content. Students will contact their teacher if they encounter a website that could be inappropriate.

Communicating Safely Online - There are many great ways to collaborate online. Either via discussion boards, posts, comments, chat, email, etc. With that collaboration, comes caution. Students will not do any of the following:

- Post private information (such as full name, address, phone number, etc) without the permission of a trusted adult;
- Share passwords or usernames;
- Post negative or harassing comments.

Gaggle: Eanes ISD implemented a new technology application to proactively protect students and ensure their safety and well-being in digital spaces. The district launched the Gaggle Safety Management solution to manage student safety on school-provided technology and further promote student and educator productivity in a safe and controlled environment.

Eanes ISD utilizes Gaggle to have the ability to analyze emails for inappropriate behavior as well as identify potential serious situations such as self-harm, cyberbullying, substance abuse, threats and more.

Digital Citizenship

The internet is a powerful community of connected people. That connection requires levels of responsibilities to one another. Part of being a good digital citizen is using technology in a responsible, appropriate way. Below are some specific areas to address with elementary-age children.

Responsible Decision Making and Self-Management - Students will have access to digital and online resources. These should be used for instructional purposes and in accordance with the student code of conduct and district policies.

Email etiquette - Students may have access to a school email account after receiving basic training on email etiquette. Please know that all email can be viewed by teachers, administrators or parents. Email should be written with thought to the audience and purpose. Abuse or misuse of district email may require disciplinary action.

Commenting Responsibility - Students will be able to make comments on age-appropriate websites or collaborative online workspaces. These comments, like anything else on the internet, have a certain amount of digital permanence. Students will display respect and thoughtfulness online by not posting comments that are negative, inappropriate, or personal about others or themselves.

Digital Footprints - Information you post on the internet can affect your future. The internet can be a powerful collaborative tool, but any information you post on it is accessible by anyone. If you have a question about posting something, you should always consult with your teacher or parent before posting.

Digital Ethics - Students will use the internet and digital tools to produce content for the classroom. Students will not present the work of others as their own work (known as plagiarism) There may be times when other students have left their own work on a computer or that students will collaborate on a digital project. Students will not delete or damage other students' work intentionally. Students will ask for permission prior to posting videos or photos of other students and staff. When working on projects or any other work with online resources, students will follow copyright and creative commons laws.

Cyberbullying - Cyberbullying is the use of digital technologies or mobile devices to harass, threaten, embarrass or torment another student. This can happen both directly and indirectly. Students will practice "think before you send" and will report any cyberbullying they become aware of to a trusted adult.

Research and Information Literacy

Searching - Students will use a variety of search engines to search for information and content. Students will understand the functions of effective keywords and categories to find useful and relevant information online.

Research and Evaluation - Students will choose websites with quality information and when possible, use multiple sources to find their information. Students will be able to identify online advertisements and spam on websites and understand the purpose behind those advertisements.

Appendix F: Responsible Use Guidelines (Middle School Students):

Eanes Independent School District Middle School Responsible Use Guidelines for Technology

Our staff and students use technology to learn. Technology is essential to facilitate the creative problem-solving, information fluency, communication and collaboration that we see in today's global economy. While we want our students to be active contributors in our connected world, we also want them to be safe, legal, and responsible. The Responsible Use Guidelines (RUG) support our vision of responsible technology use and promote a strong sense of digital citizenship. The RUG applies to all Eanes Independent School District computer networks (including the devices made available by them), and all devices connected to those networks (whether they be student owned or otherwise).

With the ability to use technology comes responsibility. It is important you read and discuss the District Responsible Use Guidelines, ask questions if you need help understanding them, and sign the agreement form. It is your responsibility to follow the rules for appropriate use. Irresponsible system use will result in the loss of the privilege of using this educational and administrative tool. Please review the leveled-guidelines following this document, which explain in greater detail responsible use expectations for elementary, middle school and high school students in the areas of Internet Safety & Security, Digital Citizenship, and Research & Information Literacy.

Please note that the Internet is a global computer network of many types of communication and information networks. It is possible that you may run across some material you might find objectionable. While Eanes ISD will use Internet filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. District provided resources are not private and may be viewed by district officials. The school district will provide you with third party accounts (such as Google Apps) that must also adhere to these Responsible Use Guidelines. Any other third party accounts that are used for educational purposes, must also adhere to these Responsible Use Guidelines. Eanes Independent School District will monitor your activity on the network and on school-issued devices.

It will be your responsibility to follow the rules for appropriate use.

RESPONSIBLE USE AND DIGITAL CITIZENSHIP

Any use described below is deemed "responsible" and consistent with the Eanes ISD Responsible Use Guidelines for Technology. The final decision regarding whether any given use of the network or technology resource is acceptable lies with the Superintendent or designee.

- Use is mainly for educational purposes, but some limited personal use is permitted. (Remember that people who receive Email from you with a District address might mistakenly infer that your message represents the District's point of view).
- Use furthers the educational and administrative purposes, goals, and objectives of Eanes ISD.
- Use is limited to your own individual account - you and only you should use that account. You should not share your password with others.
- Use furthers research related to education and instruction
- Use does not violate the student code of conduct or employee standards of conduct.
- Use of appropriate online names as well as use of polite and appropriate language/content on all online posts.
- Use of websites, content, and media is properly cited with respect to copyright.

UNACCEPTABLE AND IRRESPONSIBLE USE

Any of the following uses is deemed “unacceptable and irresponsible” and a violation of the Eanes ISD Responsible Use Guidelines for Technology. This list does not include all possible violations and supplements prohibited behaviors defined in the Student Code of Conduct. The final decision regarding whether any given use of the network or technology resource is acceptable lies with the Superintendent or designee.

Disciplinary action may be taken for unacceptable and irresponsible use of the network or Internet.

- Unauthorized use of copyrighted material, including violating district software licensing agreements
- Posting of videos or photos without permission of the individual or group.
- Sending, possessing, delivering, or posting electronic messages or images that are abusive, obscene, sexually oriented, harassing, threatening, intimidating, illegal, or that cause a material or substantial disruption at school or infringes on the rights of another student at school, including cyberbullying.
- Use of technology resources such as chat rooms, social sites, and games in a manner that causes disruption to the educational program
- Use of school technology resources to encourage illegal behavior or threaten school safety
- Use of personal device that conflicts with Board policy and/or the student handbook and code of conduct
- Use of any means to disable or bypass the district’s Internet filtering system or other security systems
- Attempting to alter, destroy, disable or gain unauthorized access to district technology equipment, district data, the data of other users, or district network resources.
- Encrypting communications or files to avoid security review
- Posting personal information about yourself or others (such as addresses and phone numbers) other than as needed to conduct school operations
- Forgery of email messages or transmission of unsolicited junk email
- Use related to commercial activities or for commercial gain
- Use that violates the student code of conduct or employee standards of conduct, or is unlawful
- Wasting school resources through the improper use of the computer and/or network systems

One or more of the following consequences may be imposed:

- Disciplinary action, in accordance with Board policy and/or the student handbook and code of conduct (as applicable)
- Removal of personal device(s) if applicable by authorized District personnel

CONSEQUENCES FOR INAPPROPRIATE USE

Internet Safety and Security

Go Places Safely and Responsibly - The internet can be a great place to discover and visit far-away places to learn new things. Staying safe online is similar to staying safe in the world. Students will choose safe, age-appropriate sites with the guidance of their teachers.

Staying Safe Online - EISD has filters in place to help steer students clear of inappropriate content; however, students may encounter some inappropriate information. Students will contact their teacher if they encounter a website that could be inappropriate.

Communicating Safely Online - Use of the internet and online collaboration is an important part of being in middle school. However, there are still risks involved when engaging in online conversation. Students will understand situations where online talk may be risky. Students will recognize and report any warning signs of online predators. Students will not participate in inappropriate dialogue with others online.

Gaggle: Eanes ISD implemented a new technology application to proactively protect students and ensure their safety and well-being in digital spaces. The district launched the Gaggle Safety Management solution to manage student safety on school-provided technology and further promote student and educator productivity in a safe and controlled environment.

Eanes ISD utilizes Gaggle to have the ability to analyze emails for inappropriate behavior as well as identify potential serious situations such as self-harm, cyberbullying, substance abuse, threats and more.

Security of Information - Sharing of information online can be a great way to accomplish a task or work on a project collaboratively. However, there are certain bits of information that students should not share online or with others. Students will not share any of the following:

- Passwords
- Private and personal information about yourself
- Private and personal information about others

Internet Privacy - Many websites collect information from visitors for advertising or data collection purposes. Students will learn and use online privacy terms. Students will understand how and why companies collect their information so they can make informed decisions before providing personal information to a website.

Digital Citizenship

The internet is a powerful community of connected people. That connection requires levels of responsibilities to one another. Part of being a good digital citizen is using technology in a responsible, appropriate way. Below are some specific areas to address with middle school children

Responsible Decision Making and Self-Management - Students will have access to digital and online resources. These should be used for instructional purposes and in accordance with the student code of conduct and district policies.

Social Media & Email - Students will have access to a school email account after receiving basic training on email etiquette. Please know that all email can be viewed by teachers, administrators or parents. Email should be written with thought to the audience and purpose. Certain online school-approved social media sites are allowed for instructional use (based on grade of the student). Students will learn about interaction, risks, and responsible use on both school-approved and other social media sites that they may encounter. Abuse or misuse of district email may require disciplinary action.

Commenting Responsibility - As the use of social media and other age-appropriate websites becomes available to middle school students, it is important for students to understand the positive and negative aspects of their digital life. Students will be able to make comments on age-appropriate websites or school-approved social media sites. These comments, like anything else on the internet, have a certain

amount of digital permanence. Students will display respect and thoughtfulness online by not posting comments that are negative, inappropriate, or personal about others or themselves.

Digital Ethics - Students will use the internet and digital tools to produce content for the classroom. Students will not present the work of others as their own work (known as plagiarism) There may be times when other students have left their own work on a computer or that students will collaborate on a digital project. Students will not delete or damage other students' work intentionally. Students will ask for permission prior to posting videos or photos of students. When working on projects or any other work with online resources, students will follow copyright and creative commons laws.

Cyberbullying - Cyberbullying is the use of digital technologies or mobile devices to harass, threaten, embarrass or torment another student. This can happen both directly and indirectly. Students will:

- Identify strategies for dealing with cyberbullying responsibly.
- Analyze and report any offensive online behavior or interactions to a trusted adult or tip line (Quick Report).
- Create positive online communities rooted in trust and respect.
- Think before you send or post.

Students will NOT:

- Publish information that is not harmful or embarrassing to others.
- Facilitate in the spreading of rumors via online platforms.
- Participate in online polls, "bash" sessions, or other communities that are harmful to others.

"Sexting" or other inappropriate online interactions - Like cyberbullying, "sexting", or the transmission of inappropriate images or messages digitally, can result in conviction in a court of law. Students will understand the role of digital technologies in relationships. Students will not actively participate in the sharing of inappropriate photos, videos and/or information of themselves or others.

Research and Information Literacy

Searching - Students will use a variety of search engines to search for information and content. Students will understand the functions of effective keywords and categories to find useful and relevant information online.

Research and Evaluation - Students will choose websites with high-quality information and when possible, use multiple sources to find their information. Students will properly cite online resources. Students will be able to identify online advertisements and spam on websites and understand the purpose behind those advertisements.

Appendix G: Responsible Use Guidelines (High School Students):
Eanes Independent School District
High School Responsible Use Guidelines for Technology

Our staff and students use technology to learn. Technology is essential to facilitate the creative problem-solving, information fluency, communication and collaboration that we see in today's global economy. While we want our students to be active contributors in our connected world, we also want them to be safe, legal, and responsible. The Responsible Use Guidelines (RUG) support our vision of responsible technology use and promote a strong sense of digital citizenship. The RUG applies to all Eanes Independent School District computer networks (including the devices made available by them), and all devices connected to those networks (whether they be student owned or otherwise).

With the ability to use technology comes responsibility. It is important you read and discuss the District Responsible Use Guidelines, ask questions if you need help understanding them, and sign the agreement form. It is your responsibility to follow the rules for appropriate use. Irresponsible system use will result in the loss of the privilege of using this educational and administrative tool. Please review the leveled-guidelines following this document, which explain in greater detail responsible use expectations for elementary, middle school and high school students in the areas of Internet Safety & Security, Digital Citizenship, and Research & Information Literacy.

Please note that the Internet is a global computer network of many types of communication and information networks. It is possible that you may run across some material you might find objectionable. While Eanes ISD will use Internet filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. District provided resources are not private and may be viewed by district officials. The school district will provide you with third party accounts (such as Google Apps) that must also adhere to these Responsible Use Guidelines. Any other third party accounts that are used for educational purposes, must also adhere to these Responsible Use Guidelines. Eanes Independent School District will monitor your activity on the network and on school-issued devices.

It will be your responsibility to follow the rules for appropriate use.

**RESPONSIBLE USE
AND DIGITAL
CITIZENSHIP**

Any use described below is deemed "responsible" and consistent with the Eanes ISD Responsible Use Guidelines for Technology. The final decision regarding whether any given use of the network or technology resource is acceptable lies with the Superintendent or designee.

- Use is mainly for educational purposes, but some limited personal use is permitted. (Remember that people who receive Email from you with a District address might mistakenly infer that your message represents the District's point of view).
- Use furthers the educational and administrative purposes, goals, and objectives of Eanes ISD.
- Use is limited to your own individual account - you and only you should use that account. You should not share your password with others.
- Use furthers research related to education and instruction
- Use does not violate the student code of conduct or employee standards of conduct.
- Use of appropriate online names as well as use of polite and appropriate language/content on all online posts.
- Use of websites, content, and media is properly cited with respect to copyright.

Any of the following uses is deemed "unacceptable and irresponsible" and a violation of the Eanes ISD Responsible Use Guidelines for Technology. This list does not include all possible violations and

**UNACCEPTABLE
AND IRRESPONSIBLE
USE**

supplements prohibited behaviors defined in the Student Code of Conduct. The final decision regarding whether any given use of the network or technology resource is acceptable lies with the Superintendent or designee.

Disciplinary action may be taken for unacceptable and irresponsible use of the network or Internet.

- Unauthorized use of copyrighted material, including violating district software licensing agreements
- Posting of videos or photos without permission of the individual or group.
- Sending, possessing, delivering, or posting electronic messages or images that are abusive, obscene, sexually oriented, harassing, threatening, intimidating, illegal, or that cause a material or substantial disruption at school or infringes on the rights of another student at school, including cyberbullying.
- Use of technology resources such as chat rooms, social sites, and games in a manner that causes disruption to the educational program
- Use of school technology resources to encourage illegal behavior or threaten school safety
- Use of personal device that conflicts with Board policy and/or the student handbook and code of conduct
- Use of any means to disable or bypass the district's Internet filtering system or other security systems
- Attempting to alter, destroy, disable or gain unauthorized access to district technology equipment, district data, the data of other users, or district network resources.
- Encrypting communications or files to avoid security review
- Posting personal information about yourself or others (such as addresses and phone numbers) other than as needed to conduct school operations
- Forgery of email messages or transmission of unsolicited junk email
- Use related to commercial activities or for commercial gain
- Use that violates the student code of conduct or employee standards of conduct, or is unlawful
- Wasting school resources through the improper use of the computer and/or network systems

One or more of the following consequences may be imposed:

- Disciplinary action, in accordance with Board policy and/or the student handbook and code of conduct (as applicable)
- Removal of personal device(s) if applicable by authorized District personnel

**CONSEQUENCES
FOR
INAPPROPRIATE USE**

Internet Safety and Security

Go Places Safely and Responsibly - The internet can be a great place to discover and visit far-away places to learn new things. Staying safe online is similar to staying safe in the world. Students will choose safe, age-appropriate sites with the guidance of their teachers.

Staying Safe Online - EISD has filters in place to help steer students clear of inappropriate content; however, students may encounter some inappropriate information. Students will contact their teacher if they encounter a website that could be inappropriate.

Communicating Safely Online - Use of the internet and online collaboration is an important part of being in high school. However, there are still risks involved when engaging in online conversation. Students will recognize and report any warning signs of online predators. Students will engage in safe online relationships and not participate in inappropriate dialogue with others online. Students will identify strangers and avoid risky online behavior. Students will report any inappropriate communication or possible online predators with a trusted adult.

Gaggle: Eanes ISD implemented a new technology application to proactively protect students and ensure their safety and well-being in digital spaces. The district launched the Gaggle Safety Management solution to manage student safety on school-provided technology and further promote student and educator productivity in a safe and controlled environment.

Eanes ISD utilizes Gaggle to have the ability to analyze emails for inappropriate behavior as well as identify potential serious situations such as self-harm, cyberbullying, substance abuse, threats and more.

Security of Information - Sharing of information online can be a great way to accomplish a task or work on a project collaboratively. However, there are certain bits of information that students should not share online or with others. Students will not share any of the following:

- Passwords
- Personal information/inappropriate photos of yourself
- Personal information/inappropriate photos of others

Internet Privacy - Many websites collect information from visitors for advertising or data collection purposes. Students will:

- Recognize and analyze online privacy terms.
- Understand the how and why companies collect their information so they can make informed decisions before providing personal information to a website.
- Guard against phishing, scamming and identity theft.

Digital Citizenship

The internet is a powerful community of connected people. That connection requires levels of responsibilities to one another. Part of being a good digital citizen is using technology in a responsible, appropriate way. Digital media plays an important role in a student's life and in our society. Below are some specific areas to address with high school students when learning how to grow their digital citizenship.

Social Media & Email - Students will have access to a school email account after receiving some basic training on email etiquette. Please know that all email can be viewed by teachers, administrators, or parents. Email should be written with thought of the audience and purpose. Certain online school-approved social media sites are allowed. Students will learn about interaction, risks, and responsible use on both school-approved and other social media sites that they may encounter. Abuse or misuse of district email or school-approved social media sites may require disciplinary action.

Commenting Responsibility - As the use of social media and other age-appropriate websites becomes available to high school students, it is important for students to understand the positive and negative aspects of their digital life. Students will recognize the importance of context in posting or viewing online images. Students will post appropriate comments in online and social communities. These comments, like anything else on the internet, have a certain amount of digital permanence and can affect reputation down the road. Students will display respect and thoughtfulness online by not posting comments that are negative, inappropriate, or personal about others or themselves.

Digital Ethics - Students will use the internet and digital tools to produce content and projects. Students will not present the work of others as their own work (otherwise known as plagiarism) Students will not intentionally delete or damage another student's digital work. Students will ask for permission prior to posting videos or photos of students or staff members online. When working on projects or any other work with online resources, students will follow copyright and creative commons laws.

Cheating - With the use of mobile devices, there may be temptation to cheat and share test or assignment information on a non-collaborative project. Students will not use technology and/or mobile devices to share confidential school content with other students.

Cyberbullying - Cyberbullying is the use of digital technologies or mobile devices to harass, threaten, embarrass or torment another student. Minors can be convicted in a court of law of being a cyberbully. This can happen both directly and indirectly. In order to avoid this students will:

- Identify strategies for dealing with cyberbullying responsibly.
- Analyze and report any offensive online behavior or interactions to a trusted adult.
- Create positive online communities rooted in trust and respect.
- Think before you send or post
- Recognize and identify factors that intensify cyberbullying, including what role they play in escalating or de-escalating online cruelty

Students will NOT:

- Publish information that is not harmful or embarrassing to others
- Facilitate in the spreading of rumors via online platforms.
- Participate in online polls, "bash" sessions, or other communities that are harmful to others.

"Sexting" or other inappropriate online interactions - Like cyberbullying, "sexting", or the transmission of inappropriate images or messages digitally, can result in conviction in a court of law. Students will understand the role of digital technologies in relationships. Students will not actively participate in the sharing of inappropriate photos, videos and/or information of themselves or others.

Research and Information Literacy

Searching - Students will use a variety of search engines to search for information and content. Students will understand the functions of effective keywords and categories to find useful and relevant information online.

Research and Evaluation - Students will choose websites with high-quality information and when possible, use multiple sources to find their information. Students will properly cite online resources. Students will be able to identify online advertisements and spam on websites and understand the purpose behind those advertisements.

SECTION 1: STUDENTS

1.1. Empowered Learner

Students leverage technology to take an active role in choosing, achieving and demonstrating competency in their learning goals, informed by the learning sciences. Students:

- 1.1.a. articulate and set personal learning goals, develop strategies leveraging technology to achieve them and reflect on the learning process itself to improve learning outcomes.
- 1.1.b. build networks and customize their learning environments in ways that support the learning process.
- 1.1.c. use technology to seek feedback that informs and improves their practice and to demonstrate their learning in a variety of ways.
- 1.1.d. understand the fundamental concepts of technology operations, demonstrate the ability to choose, use and troubleshoot current technologies and are able to transfer their knowledge to explore emerging technologies.

1.2. Digital Citizen

Students recognize the rights, responsibilities and opportunities of living, learning and working in an interconnected digital world, and they act and model in ways that are safe, legal and ethical. Students:

- 1.2.a. cultivate and manage their digital identity and reputation and are aware of the permanence of their actions in the digital world.
- 1.2.b. engage in positive, safe, legal and ethical behavior when using technology, including social interactions online or when using networked devices.
- 1.2.c. demonstrate an understanding of and respect for the rights and obligations of using and sharing intellectual property.
- 1.2.d. manage their personal data to maintain digital privacy and security and are aware of data-collection technology used to track their navigation online.

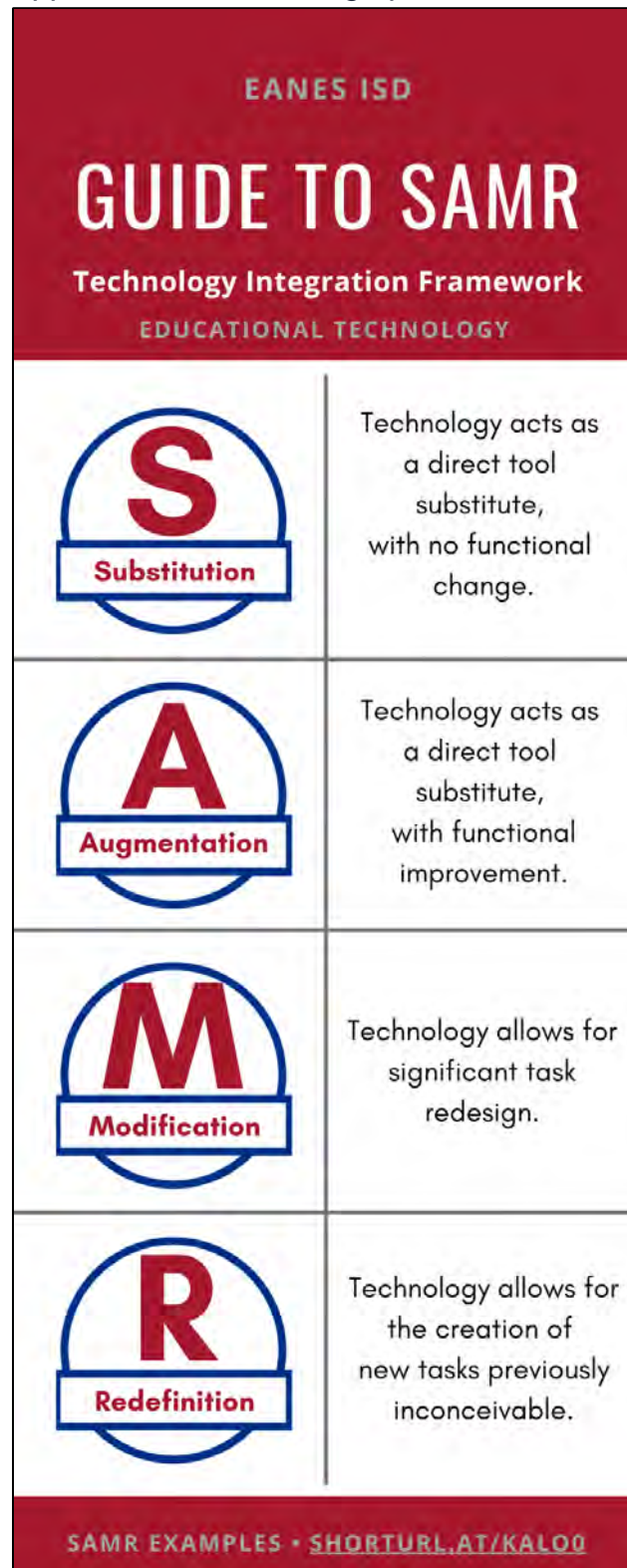
1.3. Knowledge Constructor

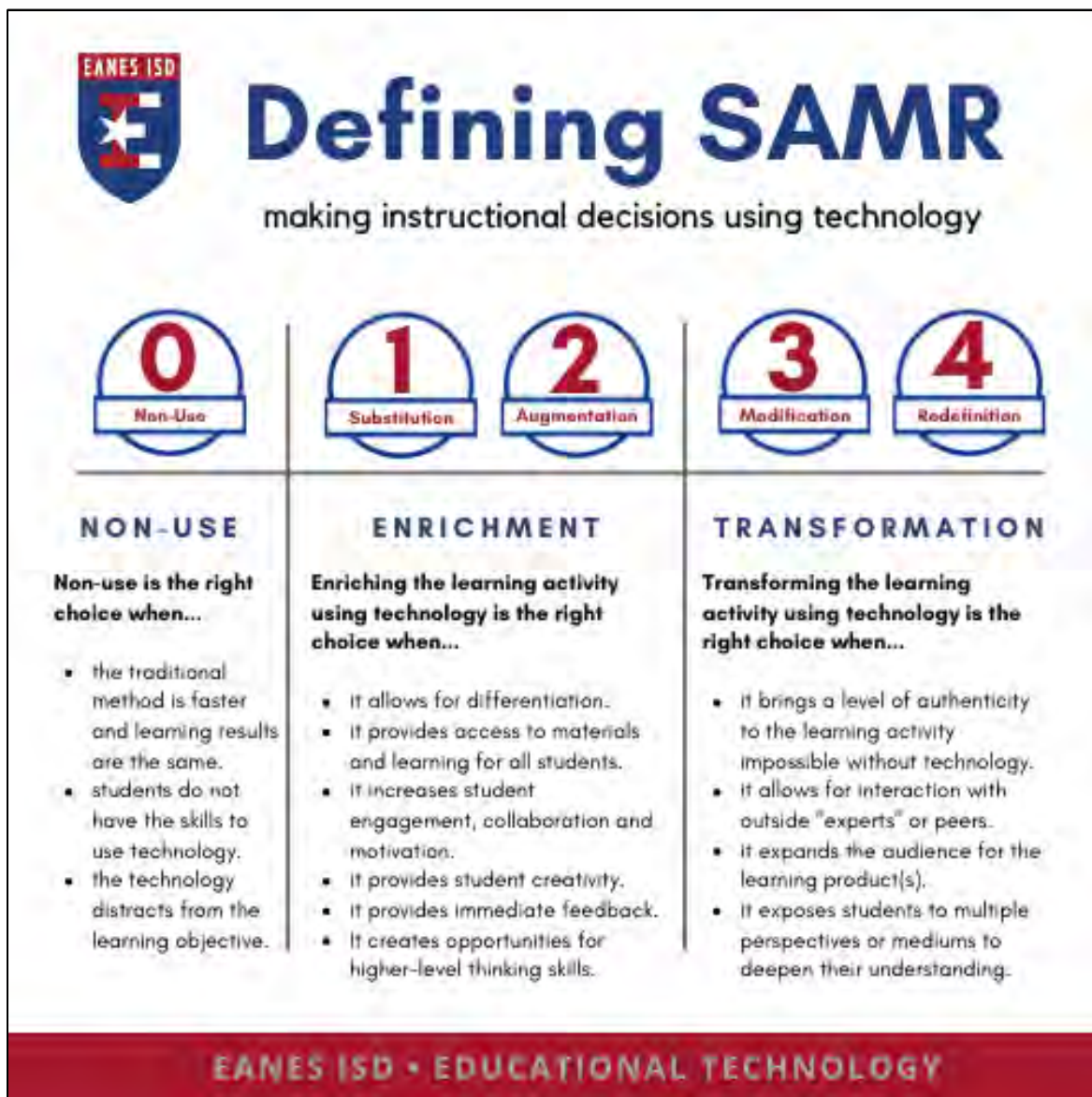
Students critically curate a variety of resources using digital tools to construct knowledge, produce creative artifacts and make meaningful learning experiences for themselves and others. Students:

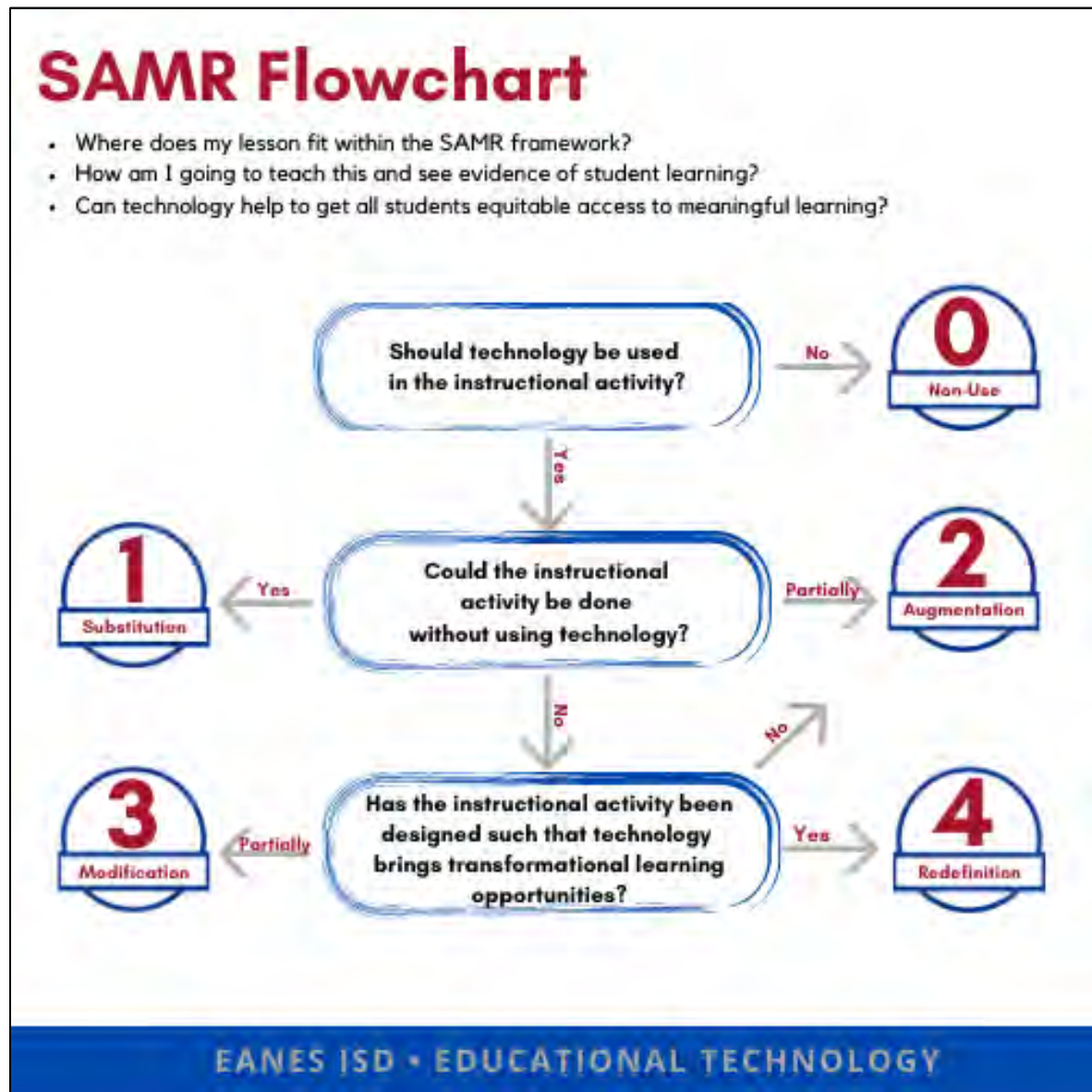
- 1.3.a. plan and employ effective research strategies to locate information and other resources for their intellectual or creative pursuits.
- 1.3.b. evaluate the accuracy, perspective, credibility and relevance of information, media, data or other resources.
- 1.3.c. curate information from digital resources using a variety of tools and methods to create collections of artifacts that demonstrate meaningful connections or conclusions.
- 1.3.d. build knowledge by actively exploring real-world issues and problems, developing ideas and theories and pursuing answers and solutions.



Appendix I: SAMR Infographic







Educational Technology

Technology Integration through UDL



ENGAGEMENT

Can **technology...**

- Make this activity/lesson fun and active?
- Have students experience real world application?
- Cause students to interact with peers?

REPRESENTATION

Can **technology...**

- Give all students access to this content?
- Provide multiple ways for a student to learn this content or skill?
- Give students the opportunity to practice new learning?
- Connect students to subject-matter experts?



ACTION & EXPRESSION

Can **technology...**


- Provide different ways that students could show their mastery of the concept or skill?
- Allow for real-world application of the new learning or skills?






Appendix M: IMS Global: TrustED App Dashboard Rubric


4/22/22, 10:33 AM


Compatibility Check: Google Forms - Vettings

 **Eanes Independent School District**


 **Kristy Sailors**
Chief Technology Officer



 **Google Forms**
By Google LLC




 **PREFERRED**

CONTRIBUTING MEMBER





 **App Vetting**

App Vetting Profile
02/06/2022 by **Kevin Lewis**, Project Manager at IMS Global

Regulatory Compliance

 **UNKNOWN**  **NO**  **YES**

The information below provides insight into compliance with various regulatory policies.

| | |
|--------------------------------|---|
| GDPR Compliant |  |
| FERPA Compliant |  |
| COPPA Compliant |  |
| Approved for children under 13 |  |

Policies Cited

The following urls were cited as a basis for this information

Terms of Service/Terms of Use
<https://policies.google.com/terms?hl=en>

Privacy Policy
https://edu.google.com/why-google/privacy-security/?modal_active=none

Cookie Policy

<https://app.ledtech.org/district/trustedapps/1962/vettings/0>

1/6

<https://policies.google.com/technologies/cookies?hl=en-US>
Security Practices
https://edu.google.com/why-google/privacy-security/?modal_active=none
Rubric Results

N/A UNMET PARTIAL MEETS



DATA COLLECTION



SECURITY



THIRD PARTY DATA



ADVERTISING

Rubric Area**Expectations****Notes**

Meets

Partially

Unmet

GENQ1 How are changes to key policies managed?

ANSWER: Notification is provided to the user in advance and a history of policy revisions are available

DCQ1 Do the policies list all data collected?

ANSWER: Policies list the data collected OR policies state no data is collected

DCQ2 Do the policies indicate how data is collected?

ANSWER: Policies state specifically how data is collected OR policies state no data collected

DCQ3 Do the policies state who owns the data?

ANSWER: Policies state the user owns the data alone OR policies state no data collected


DATA COLLECTION



DCQ4 Do the policies allow users to delete their data entirely?

ANSWER: Policies allow users to delete data entirely after a period of time OR policies state no data collected



DCQ5 Do the policies state the retention of data?

ANSWER: Policies have a 60-day or less retention policy OR policies state no data collected



SECQ1 Do the policies state how data is protected?

ANSWER: Policies list the steps taken to protect data or OR policies state no data collected



SECQ2 Do the policies state all confidential & sensitive information is encrypted throughout?

ANSWER: Data encrypted throughout OR passes an encryption test with no vulnerabilities OR policies state no data collected



SECQ3 Do the policies state whether or not it enforces strong password creation?

ANSWER: Supplier enforces strong password creation OR supplier user base exempt from password requirements or OR no account creation required



SECQ4 Do the policies indicate whether or not it leverages 2 step (or other forms of multifactor)





THIRD PARTY DATA

authentication?

ANSWER: Supplier uses SSO or an LTI launch OR no account creation is required OR supplier user base exempt from 2-step authentication requirements

SECQ5 Do the policies state the use of cookies?

ANSWER: Policies list all cookies used and each cookie's purpose OR policies state that it only uses cookies that are crucial for app functionality

SHRQ1 Do the policies state the use of third parties?

ANSWER: Policies list each third party separately OR policies state third party use strictly for app functionality OR policies state that they do not use third parties

SHRQ2 Do the policies state what information is shared with each third party?

ANSWER: Policies list the data it shares with each third party separately OR policies state that it does not share any data with any third party

SHRQ3 Do the policies state whether or not users can opt out of third party data sharing?

ANSWER: Policies include an easy opt out process for users OR policies state that it does not share any data with any third party

SHRQ4 Do the policies state if the supplier requires third parties to adhere to the terms of

the vendor/customer agreement?

ANSWER: Supplier claims responsibility for third party privacy practices OR policies state that it does not share any data with any third party

SHRQ5 Do the policies state whether or not user is notified of a change in third parties?

ANSWER: Supplier changes third party and keeps the same data sharing terms OR supplier does not use any third parties

ADVQ1 Do the policies indicate if advertisements are displayed?

ANSWER: No ads are displayed

ADVQ2 Do the policies indicate whether or not users are targeted for advertisement?

ANSWER: Policies guarantee no ad targeting OR policies state no ads are used on its platform

ADVQ3 Do the policies indicate whether or not any third parties track or collect information for advertisement?

ANSWER: Policies state third parties are not used for ads or tracking

ADVQ4 Do the policies indicate whether or not web beacons or other tracking methods are used for ad purposes?

ANSWER: Policies state that it only tracks interactions within

4/22/22, 10:33 AM

Compatibility Check: Google Forms - Vetting

its application OR policies state that it does not use any tracking technologies for ads

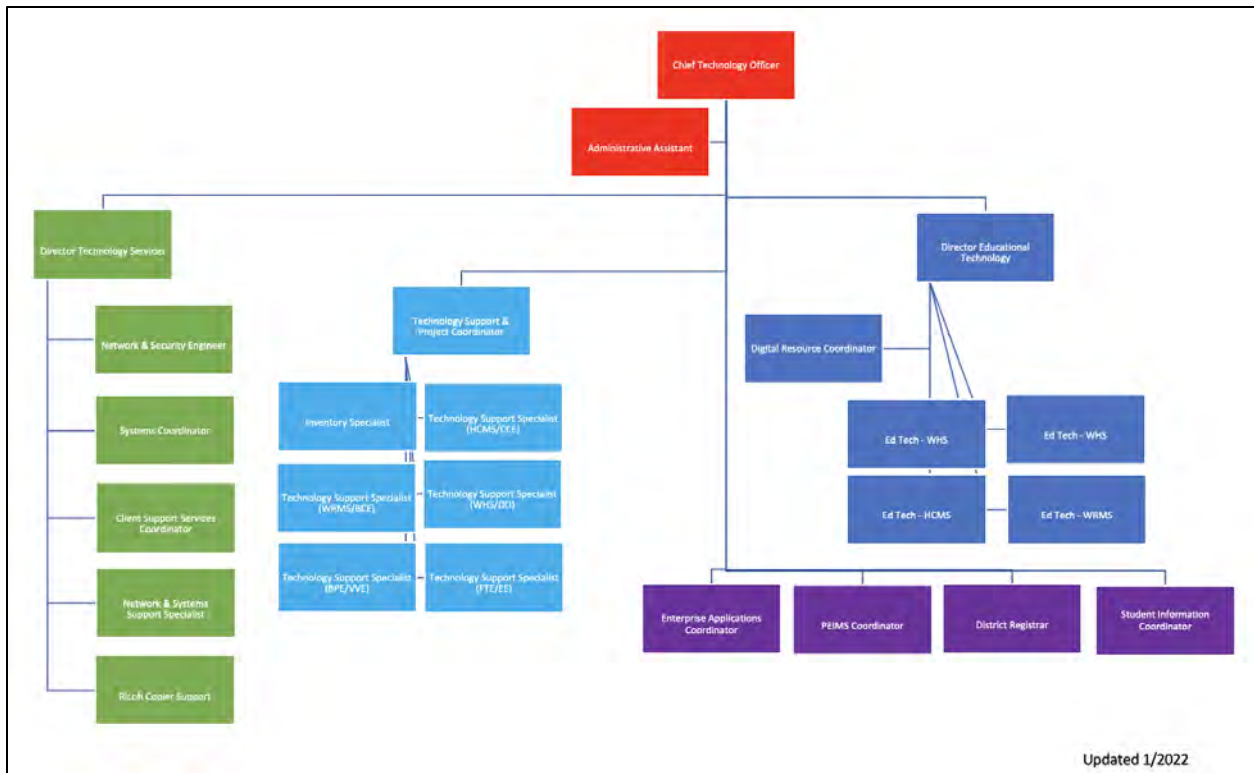
ADVQ5 Do the policies state whether or not users can opt out of sharing data with advertisers?

ANSWER: Policies state in detail how users can opt out of sharing data with advertisers OR policies state no ads are used on its platform

© 2019 - 2022 IMS Global Learning Consortium Inc. All Rights Reserved.

Terms of Service

Appendix N: Technology Services Organizational Chart



VENDOR AGREEMENT

THIS VENDOR AGREEMENT ("Agreement") is made and entered into on the Effective Date, as hereinafter defined, by and between _____ ("Vendor"), and **Eanes ISD** ("Owner"), for provision of:

NOW, THEREFORE, in consideration of the mutual promises and covenants hereinafter set forth, and for other good and valuable consideration, the sufficiency of which is hereby acknowledged and the receipt of which shall be acknowledged by endorsement thereof, the parties do hereby agree as follows:

1. **Services to be Performed by Vendor**—The terms of this Agreement incorporate by reference the provisions stated in the Proposal attached hereto as **Exhibit A to this Agreement** ("Proposal"). Vendor shall perform the services described in the Proposal according to the standards of his profession.
2. **Compensation**—In consideration of the product provided and/or services performed by Vendor under this Agreement, Vendor shall receive from Owner a sum of up to _____ (\$ _____).
Is the dollar amount over **\$75,000**? Yes No
3. **Time of Completion** - Vendor shall include beginning and ending dates of the services performed in **Exhibit A to this Agreement** "Proposal").
4. **Relationship of the Parties**—It is understood and agreed that Vendor is an independent contractor and neither Vendor nor any employees, volunteers, or agents contracted by Vendor shall be deemed for any purposes to be employees, volunteers or agents of Owner. Vendor shall assume full responsibility for the action of such employees, volunteers, or agents while performing any services incident to this Agreement, and shall remain solely responsible for their supervision, daily direction and control, payment of salary (including withholding of income taxes and social security), workers' compensation, disability benefits and like requirements and obligations.
5. **No Waiver of Immunity**—Owner does not waive or relinquish any immunity or defense on behalf of itself, its trustees, officers, employees, and agents as a result of its execution of this Agreement and performance of the functions or obligations described herein.
6. **Insurance and Indemnity**—Vendor agrees to indemnify and hold harmless Owner, its trustees and employees against any and all losses, costs, expenses and liabilities, including but not limited to reasonable attorneys' fees and court costs, to the extent they arise out of Vendor's acts or omissions.
Only to the extent required by law, Owner agrees to indemnify and hold harmless Vendor and its direct employees against any and all losses, costs, expenses and

liabilities, including but not limited to reasonable attorneys' fees and court costs, to the extent they arise out of Owner's acts or omissions.

7. **Compliance with Laws**—Vendor shall maintain any and all applicable license(s) and certification(s) necessary to perform any services contemplated by this Agreement. Vendor shall observe and comply with all Federal, State, County and local laws, and Owner's Board Policies that in any manner affect the provision of services and performance of all obligations undertaken pursuant to this Agreement.
8. **Authorization of Agreement**—Each party represents and warrants to the other that execution of this Agreement has been duly authorized, and that this Agreement constitutes a valid and enforceable obligation of such party according to its terms.
9. **No Waiver**—No waiver of a breach of any provision of this Agreement shall be construed to be a waiver of any breach of any other provision. No delay in acting with regard to any breach of any provision shall be construed to be a waiver of such breach.
10. **Notices**—Any notice required or permitted to be given under this Agreement shall be in writing, and shall be deemed to have been given when delivered by email. Notices shall be addressed as follows:

VENDOR: _____

By: _____

Printed Name & Title: _____

Date: _____

EANES INDEPENDENT SCHOOL DISTRICT

By: _____

Printed Name & Title: _____

Date: _____

Any party may designate a different address by giving the other party ten (10) days written notice in the manner provided above.

11. **No Assignment**—No assignment of this Agreement, or any duty or obligation of performance hereunder, shall be made in whole or in part by either party without the prior written consent of the other party.
12. **Amendments**—This Agreement may be amended or modified by, and only by, a written instrument approved by the Owner in accordance with Owner's Board Policy.

13. **Termination**—Owner may terminate this Agreement with or without cause upon thirty (30) days written notice to Vendor. Vendor shall be entitled to compensation for all services provided up to the effective date of termination.
14. **Section Headings**—The headings of sections contained in this Agreement are for convenience only, and they shall not, expressly or by implication, limit, define, extend or construe the terms or provisions of the sections of this Agreement.
15. **Governing Law**—This Agreement is made in Texas and shall be construed, interpreted, and governed by Texas law. The parties shall consent to the jurisdiction and venue of the courts of Travis County, Texas, for any action under this Agreement.
16. **Complete Understanding**— This Agreement and all Exhibits, Supplements and Amendments thereto shall constitute the complete understanding of Vendor and Owner. This Agreement constitutes the sole and only agreement of the parties to it and supersedes any prior understandings or written or oral agreements between the parties respecting the subject matter of this Agreement. Any terms, conditions or limitations of warranty/liability contained in Vendor's Proposal are not included, and are hereby expressly excluded from this Agreement unless such terms, conditions or limitations are restated in the main body of this Agreement. The appearance of such matters in any Exhibit to this Agreement is ineffective, as the inclusion of Vendor's proposal is intended to only provide information relating to the scope, deliverables, deadlines and fees relating to Vendor's services.
17. **Effective Date**—The “Effective Date” of this Agreement shall be _____ , the date that all necessary and authorized representatives of Owner have endorsed the same.

VENDOR

**EANES INDEPENDENT
SCHOOL DISTRICT**

Signature

Signature

Printed Name and Title

Printed Name and Title

Eanes ISD Secretary:

Attach Proposal -

Attach Certificate of Insurance (ACORD):

Attach Completed HB 1295 -

Purchasing:

EANES ISD DATA PROTECTION AGREEMENT (“DPA”)

This DPA is made by and between _____ (“Contractor”) and Eanes Independent School District (“EISD”) as a condition of Contractor’s, its employees’ and agents’ (including subcontractors) access to, and use, maintenance, and disclosure of, District Data (as defined below) in connection with Contractor’s provision of products and services (collectively, “Services”) to EISD. This DPA is hereby made part of any agreement(s) between the parties with respect to the Services (each, an “Agreement”), notwithstanding any merger/integration or similar provision contained in any such Agreement(s), and Contractor and EISD agree as follows:

1. “District Data” means all information, including, but not limited to, business, administrative, financial, student, and personnel information, work product, and other intellectual property that is: (1) created by EISD, its employees, contractors, agents, affiliates, students, parents, and users, or provided or otherwise made available to Contractor, its employees and agents by EISD, its employees, contractors, agents, affiliates, students, parents, and users through the Services or otherwise in connection with the Services; or (2) gathered by Contractor, its employees and agents through the Services or other means (e.g., Contractor technology) in connection with the Services. District Data includes, but is not limited to, any information that is protected by law, such as “personally identifiable information” and student “education records” as those terms are defined under the Family Educational Rights and Privacy Act, 20 USC 1232g, as amended (“FERPA”). District Data does not include “de-identified” information as that term is defined by the U.S. Department of Education for purposes of FERPA.

2. All rights in and to District Data shall remain the sole and exclusive property of EISD. Contractor has no rights, implied or otherwise, in District Data, except as expressly stated in this DPA.

3. EISD hereby authorizes Contractor to access, use, and maintain District Data, and disclose District Data to its employees and agents, solely as reasonably necessary to provide Services to EISD, subject to the requirements of applicable law and this DPA. Contractor shall ensure that its employees and agents agree to comply with data protection obligations similar to, and in no event less restrictive than, those applicable to Contractor under this DPA and applicable law. Except as required by law or authorized by EISD in writing, Contractor, its employees and agents shall not disclose District Data to any third party. EISD shall have access to District Data at all times.

4. Contractor shall comply with all laws applicable to the access to, and use, maintenance, and disclosure of, District Data. Contractor acknowledges that it has been designated a school official with legitimate educational interests in any FERPA-protected information contained in District Data and agrees to abide by any requirements imposed by law on school officials. The parties agree that: (1) the Services are services/functions for which EISD would otherwise use its own employees; (2) Contractor meets the criteria in EISD's annual notification of FERPA rights for being a school official in connection with the Services; (3) Contractor is under EISD's direct control with respect to its access to, and use, maintenance, and disclosure of, FERPA-protected information; and (4) Contractor will access, use, maintain, and disclose FERPA-protected information only for the purpose for which it was disclosed and will not re-disclose such information to other parties unless Contractor has specific written authorization from EISD to do so and it is otherwise permitted by FERPA. EISD parents/guardians and students shall not be required to waive any FERPA rights in connection with the Services, and any such waiver shall be null and void.

5. Contractor shall use commercially reasonable security procedures and practices to preserve the confidentiality, integrity, and availability of District Data and protect it from unauthorized acquisition, access, use, or disclosure. Such measures shall be no less protective than those used to secure Contractor’s own data of a similar type. District Data shall not be stored outside the United States without EISD’s prior written consent. If Contractor suspects that District Data has been exposed to unauthorized acquisition, access, use, or disclosure, except as prohibited by law, Contractor shall immediately notify EISD, investigate the incident, and cooperate fully with EISD’s response to the incident.

6. Except as prohibited by law, Contractor shall notify EISD of any legal order or other demand seeking District Data prior to disclosing District Data in response thereto, and Contractor shall reasonably cooperate with EISD's efforts, if any, to protect District Data.

7. Contractor will promptly notify EISD of any change in Contractor's, its employees' or agents' circumstances that are reasonably expected to materially affect District Data, including, but not limited to, any assignment, transfer, or cessation of business or unlawful conduct, and shall reasonably cooperate with EISD's requests related thereto. This DPA shall be binding upon, and inure to the benefit of, Contractor's permitted successors and assigns, if any.

8. Upon the termination of any Services, or as otherwise requested by EISD in writing, Contractor shall ensure that: (a) all applicable District Data is promptly transferred to EISD as reasonably requested by EISD; and (2) all applicable District Data in Contractor's, its employees' and agents' possession is destroyed in a commercially reasonable manner (unless Contractor is expressly permitted by law to retain such District Data). Notwithstanding the termination of the Services or any Agreement(s), this DPA shall continue in full force and effect until all District Data in Contractor's, its employees' and agents' possession has been securely destroyed as required herein.

9. A material breach of this DPA shall constitute a material breach of the applicable Agreement(s), if any. Upon a material breach of this DPA, EISD may suspend or terminate Contractor's, its employees' and agents' access to District Data. If Contractor fails to cure such breach as provided under the applicable Agreement(s), if any, or within ten (10) days after receiving written notice thereof, whichever is later, EISD may terminate the Services and any applicable Agreement(s), without penalty, liability, or further obligation. The foregoing remedies shall be in addition to and without limitation of any other rights or remedies of EISD.

10. This DPA shall be governed by Texas law, without regard to choice of law principles. The mandatory and exclusive venue for any dispute related to this DPA shall be in the state or federal courts for Travis County, Texas, and the parties hereby consent to the jurisdiction of said courts.

11. In the event of a conflict between or among this DPA, any Agreement(s), and/or applicable law, the requirement that affords the most protection to District Data shall supersede and control.

IN WITNESS THEREOF, the Parties have executed this DPA effective _____, 20__.

CONTRACTOR: _____

By: _____
Name: _____
Title: _____

EXHIBIT A to DATA PROTECTION DPA

Other types or categories of District Data:

List Inserted: Yes No

**You MUST check off at least one box and/or add description under
"Other types or categories of District Data" before signing.**

VENDOR: _____

Signature: _____

Print Name: _____

Title: _____

Date: _____

[INSERT LIST, DATA FIELD, ETC. OR "None"]

EISD SOFTWARE AGREEMENT

EANES INDEPENDENT SCHOOL DISTRICT (hereafter, “EISD”) and _____
(hereafter, “Vendor”) hereby enter into this Software Agreement (hereafter, “Agreement”) on the following terms:

1. **Agreement Documents:** The term “Agreement” as used herein shall include the following Agreement Documents, which are incorporated herein by reference for all purposes, and in the event of a conflict or inconsistency, the Agreement Documents shall be given precedence as follows:
 - a. The body of this EISD Software Agreement;
 - b. The attached Data Protection Addendum (“DPA”);
 - c. Exhibit A – [*Pricing Schedule*];
 - d. Exhibit B – [*Service Schedule/Scope of Work/Description/Specifications*];
 - e. Exhibit C – [*Support and Service Level Agreement*];
 - f. Exhibit D – [*Vendor’s End User License Agreement or other terms and conditions*];
 - g. [*Applicable District RFP Document*]; and
 - h. Vendor’s proposal submitted in response to [*Applicable District RFP Document*].

During the course of providing Services, should any conflict be identified between, among, or in the Agreement Documents that cannot be resolved by the order of precedence set forth above, the Vendor shall be deemed to have agreed to the lowest pricing, the greater quantity or better quality of the Services, or the requirement most favorable to EISD.

2. **Services:** Vendor shall provide the products and services set forth in Exhibit A and further described in in Exhibits B and C (collectively, “Services”). Any software included in the Services is referred to herein as “Software.” Upon delivery of the Software to EISD, Vendor shall also deliver copies of Vendor’s standard user manuals, training materials, job aids, and other Vendor-provided documentation and materials (collectively, “Documentation”), which shall be subject to the terms of this Agreement. Vendor shall promptly provide maintenance and support services, including telephone and email support, bug fixes, and updates and upgrades to the Software in accordance with Exhibit C. Upon delivery to EISD, any updates or upgrades to the Software shall become part of the Software and will be subject to the terms of this Agreement.
3. **Term of Agreement:** The initial term of this Agreement is for a period of one (1) year [*add implementation/deployment time, if applicable*], beginning on _____ and ending on _____ (“Initial Term”) unless terminated earlier pursuant to the terms of this Agreement, with EISD having the option to renew this Agreement for up to _____ additional years in _____ [*month/year*] increments (each, a “Renewal Term”) by providing written notice of renewal to Vendor at least thirty (30) days prior to the expiration of the then-current Term. Notwithstanding the foregoing, to the extent that this Agreement includes a perpetual license to any Software or other intellectual property, this Agreement shall continue in full force and effect as to such Software or other intellectual property until terminated in accordance with the terms hereof. The phrase “Term” in this Agreement shall mean the then-current Term of the Agreement, whether the Initial Term or a Renewal Term, if any.
4. **Reservation of Rights; Grant of License:** Except as otherwise provided in this Agreement, as between Vendor and EISD, all right, title, and interest, including all intellectual property rights, in and to the Software and Documentation shall remain the sole and exclusive property of Vendor, and Vendor hereby grants EISD a nonexclusive license, as further detailed in Exhibit D, to access and use the Software and Documentation for the purposes and business of EISD during the Term of this Agreement. Vendor further grants EISD a nonexclusive license to reproduce, distribute, and use copies of the Documentation for EISD’s internal business and educational purposes during the Term of this Agreement.
5. **EISD Resources:** During the Term of this Agreement, EISD agrees to provide access to EISD staff, facilities, systems, and data to Vendor to the extent reasonably necessary for Vendor’s performance of the Services.

6. **Use Restrictions:** Except as otherwise expressly stated in this Agreement or required by law, EISD will comply with Vendor's reasonable use restrictions regarding the Software as set forth in Exhibit D; provided that any additional charges imposed upon EISD, any modification(s) to the Services, and any imposition of liability upon EISD or limitation of EISD's rights or remedies (including any mediation or arbitration requirements) under Exhibit D or any documents referenced therein, or any amendment(s) thereto, shall be ineffective unless reproduced in the body of this EISD Software Agreement. EISD shall also use reasonable efforts, including enforcement of EISD's acceptable use policies and the like, to ensure EISD end users' compliance with such restrictions; provided that nothing in this Agreement shall be construed as requiring EISD to assume liability for the acts or omissions of any third party, including EISD trustees, officers, employees, contractors, students, and other affiliates or end users.
7. **Acceptance Criteria:** EISD will not be deemed to have accepted any Services provided hereunder until such Services have been delivered to EISD in strict accordance with the requirements of this Agreement and a duly authorized employee of EISD indicates acceptance of such Services in writing.
8. **Compensation:** Vendor agrees to provide the Services, upon the terms and conditions set forth in this Agreement, for the compensation set forth in Exhibit A, up to a maximum contract amount not to exceed \$ _____ without a valid amendment to this Agreement, including any required approvals by EISD's administration and Board of Trustees. The compensation set forth herein is all-inclusive; no additional payment or reimbursement will be made. Vendor shall be solely responsible for any and all travel and other business or miscellaneous expenses incurred by Vendor in rendering the Services.
9. **Payment Terms:** All prices shall be F.O.B. destination. The prices set forth in Exhibit A shall not be subject to increase during the first ____ years of this Agreement. If Vendor intends to increase the prices set forth in Exhibit A for any Renewal Term(s) following the first ____ years of this Agreement, Vendor shall provide written notice to EISD of any such increase at least ninety (90) days prior to the commencement of the affected Renewal Term(s), and if EISD chooses to proceed with the renewal, the mutually agreed prices for the affected Renewal Term(s) shall be memorialized in a properly executed amendment to this Agreement. Vendor may invoice EISD for Services only after such Services have been provided and duly accepted by EISD, except that Vendor may invoice EISD for Software licensing or subscription fees upon the commencement of the applicable Software license or subscription term to the extent expressly agreed in Exhibit A. Before invoicing EISD for Services, Vendor will complete and submit an Internal Revenue Service ("IRS") Form W-9. Vendor shall submit detailed, itemized invoices for Services provided to EISD at the intervals agreed in Exhibit A describing the Services rendered, the dates and times when such Services were performed, and the amount due. Payment for undisputed invoices will be made by EISD within forty-five (45) days after receipt of invoice. Nothing in this Agreement or any action or inaction by EISD, including EISD's payment for Services, shall constitute a waiver by EISD of any billing dispute in connection with the Services.
- EISD is tax-exempt and shall provide proof of such status to Vendor upon reasonable request. EISD shall not be liable for any taxes in connection with this Agreement, except where otherwise required by law. Vendor shall be solely responsible for any and all applicable social security and personal income taxes and any taxes or fees measured by or imposed upon Vendor's income which may become due as a result of any payments made by EISD hereunder, and Vendor shall indemnify and hold EISD harmless in this regard.
- In the event that this Agreement is terminated prior to the end of the applicable Term, payments will only be made to the extent that Services have been performed and delivered satisfactorily to EISD in accordance with the requirements of this Agreement prior to termination and are undisputed.
10. **Change Orders:** Subject to [*Applicable District RFP Document*], any necessary approvals by EISD's administration and Board of Trustees, and applicable law, the parties may agree to modify the scope of Services under this Agreement. EISD may request that Vendor modify the Services by submitting a written proposed change order to Vendor. Vendor shall negotiate in good faith regarding change order pricing, and such pricing shall not exceed the rates set forth in Exhibit A and Vendor's proposal submitted in response to [*Applicable District RFP Document*]. Such change order will become part of this Agreement only if memorialized in a valid amendment to this Agreement in accordance with Section 37, below. If Vendor

acts on the direction of an EISD employee that is not authorized to make changes or otherwise modifies the scope of Services without a valid amendment to this Agreement, Vendor does so at its own risk or peril and risks termination of this Agreement for cause.

11. **Intellectual Property:** Vendor represents and warrants that it has all necessary rights, title, and interest in any intellectual property to be provided or otherwise made available to EISD as set forth in this Agreement. In the event of a breach of the foregoing warranty, without limiting any rights or remedies of EISD under this Agreement or applicable law, Vendor, at its own expense, shall, as reasonably agreed by the parties, promptly: (1) secure for EISD the right to continue using such intellectual property; (2) replace or modify such intellectual property to make it noninfringing, provided such replacement or modification shall not materially diminish the Services as required under this Agreement; or (3) terminate this Agreement, in whole or in part, and refund to EISD an equitable portion of any fees, including, but not limited to, any license, subscription, hosting, and maintenance fees, paid by EISD for the affected Services.
12. **VENDOR'S REPRESENTATIONS AND WARRANTIES: IF VENDOR IS A BUSINESS ENTITY, IT REPRESENTS THAT: (I) IT IS DULY ORGANIZED, VALIDLY EXISTING AND IN GOOD STANDING UNDER THE LAWS OF THE STATE OF ITS ORGANIZATION; (II) IT IS AUTHORIZED AND IN GOOD STANDING TO CONDUCT BUSINESS IN THE STATE OF TEXAS; (III) IT HAS ALL NECESSARY POWER AND HAS RECEIVED ALL NECESSARY APPROVALS TO EXECUTE AND PERFORM ITS OBLIGATIONS IN THIS AGREEMENT; AND (IV) THE INDIVIDUAL EXECUTING THIS AGREEMENT ON BEHALF OF VENDOR IS AUTHORIZED TO DO SO.**

VENDOR WARRANTS THAT ALL GOODS AND SERVICES FURNISHED UNDER THIS AGREEMENT WILL CONFORM IN ALL RESPECTS TO THE TERMS OF THIS AGREEMENT, INCLUDING ANY SPECIFICATIONS, STANDARDS, AND DOCUMENTATION INCORPORATED HEREIN, INCLUDING, WITHOUT LIMITATION, THOSE DETAILED IN [APPLICABLE DISTRICT RFP DOCUMENT].

VENDOR WARRANTS THAT ALL GOODS PROVIDED BY VENDOR UNDER THIS AGREEMENT WILL BE FREE FROM DEFECTS IN MATERIAL, WORKMANSHIP, AND DESIGN FOR THE LONGER OF ONE (1) YEAR FOLLOWING EISD'S ACCEPTANCE OF SUCH GOODS OR THE APPLICABLE WARRANTY PERIOD OTHERWISE SET FORTH IN THIS AGREEMENT. VENDOR WARRANTS THAT ALL GOODS PROVIDED BY VENDOR UNDER THIS AGREEMENT ARE SUITABLE FOR AND WILL PERFORM IN ACCORDANCE WITH THE PURPOSES FOR WHICH THEY ARE INTENDED.

VENDOR FURTHER WARRANTS THAT, DURING THE TERM OF THIS AGREEMENT, ANY SOFTWARE PROVIDED BY VENDOR HEREUNDER WILL PERFORM SUBSTANTIALLY IN ACCORDANCE WITH THE SPECIFICATIONS SET FORTH IN VENDOR'S PROPOSAL SUBMITTED IN RESPONSE TO [APPLICABLE DISTRICT RFP DOCUMENT] AND ANY SPECIFICATIONS OR OTHER DOCUMENTATION PROVIDED TO EISD BY VENDOR IN CONNECTION WITH THIS AGREEMENT OR THE SERVICES.

VENDOR WARRANTS THAT ANY PROFESSIONAL SERVICES OR OTHER WORK PERFORMED BY VENDOR IN CONNECTION WITH THIS AGREEMENT OR THE SERVICES WILL BE PERFORMED USING COMMERCIALY REASONABLE SKILL AND CARE, AND BE OF A PROFESSIONAL QUALITY CONSISTENT WITH GENERALLY ACCEPTED INDUSTRY STANDARDS AND PRACTICES.

TO THE EXTENT THAT THE SERVICES INCLUDE ANY THIRD-PARTY GOODS OR SERVICES, IN ADDITION TO VENDOR'S WARRANTIES HEREINDER, VENDOR HEREBY TRANSFERS TO EISD, TO THE EXTENT TRANSFERABLE, WHATEVER WARRANTIES AND INDEMNITIES VENDOR RECEIVES FROM THE MANUFACTURER, PRODUCER, OR OTHER PROVIDER OF ANY SUCH GOODS OR SERVICES, INCLUDING ANY TRANSFERABLE WARRANTIES AND INDEMNITIES RESPECTING INFRINGEMENT.

VENDOR AGREES TO TAKE COMMERCIALLY REASONABLE ACTION TO ASSIST EISD IN PURSUING ANY AVAILABLE REMEDIES UNDER OR OTHERWISE ENFORCING ANY SUCH WARRANTIES AND INDEMNITIES.

WITHOUT LIMITING ANY REMEDIES OTHERWISE AVAILABLE TO EISD UNDER THIS AGREEMENT OR APPLICABLE LAW, IF ANY SERVICES DO NOT CONFORM TO THE REQUIREMENTS OF THIS AGREEMENT, EISD MAY (I) REQUIRE VENDOR TO PROMPTLY PROVIDE THE SERVICES AGAIN IN CONFORMITY WITH SUCH REQUIREMENTS, WITH NO ADDITIONAL CHARGE TO EISD; (II) EQUITABLY REDUCE PAYMENT DUE TO VENDOR TO REFLECT THE REDUCED VALUE OF THE SERVICES PROVIDED; OR (III) TERMINATE THIS AGREEMENT, IN WHOLE OR IN PART, WITHOUT PENALTY, LIABILITY, OR FURTHER OBLIGATION, AND RECEIVE A REFUND OF AN EQUITABLE PORTION OF ANY FEES, INCLUDING, BUT NOT LIMITED TO, ANY LICENSE, SUBSCRIPTION, HOSTING, AND MAINTENANCE FEES, PAID BY EISD FOR THE AFFECTED SERVICES.

VENDOR SHALL NOT LIMIT, EXCLUDE, OR DISCLAIM ANY WARRANTY(IES) OR INDEMNIFICATION OBLIGATIONS CONTAINED HEREIN OR ANY WARRANTY(IES) IMPLIED BY LAW, AND ANY ATTEMPT TO DO SO SHALL BE WITHOUT FORCE OR EFFECT.

- 13. INDEMNITY: VENDOR SHALL INDEMNIFY, HOLD HARMLESS AND DEFEND EISD AND EACH OF ITS RESPECTIVE PAST, PRESENT, AND FUTURE TRUSTEES, OFFICERS, EMPLOYEES, AND AGENTS IN THEIR INDIVIDUAL AND OFFICIAL CAPACITIES, FROM AND AGAINST ANY AND ALL CLAIMS, DEMANDS, COSTS, FINES, CIVIL PENALTIES, LOSSES OR DAMAGES, INCLUDING ATTORNEY'S FEES, COURT COSTS, AND EXPENSES, INCURRED BY EISD AND ITS TRUSTEES, OFFICERS, AGENTS, AND EMPLOYEES FOR INJURY TO PERSONS OR DAMAGE TO OR DESTRUCTION OF PROPERTY AND DEMANDS OR CAUSES OF ACTION OF WHATEVER KIND OR NATURE ASSERTED BY ANY THIRD PARTY, BASED UPON, RESULTING FROM, ARISING OUT OF, OR IN ANY WAY INCIDENT OR RELATED TO ANY ACT, ERROR, OMISSION, MISREPRESENTATION, OR MISCONDUCT OF VENDOR OR ITS EMPLOYEES, AGENTS, OFFICERS, OR SUBCONTRACTORS IN CONNECTION WITH THE PERFORMANCE OF THIS AGREEMENT OR THE SERVICES.**

VENDOR'S INDEMNIFICATION OBLIGATIONS HEREUNDER SHALL APPLY TO ANY CLAIM ALLEGING THAT ANY PORTION OF ANY INTELLECTUAL PROPERTY PROVIDED OR MADE AVAILABLE TO EISD BY VENDOR, ITS EMPLOYEES, AGENTS, OFFICERS, OR SUBCONTRACTORS IN CONNECTION WITH THIS AGREEMENT INFRINGES A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS, INCLUDING U.S. COPYRIGHT, PATENT, OR TRADEMARK.

TO THE EXTENT THAT VENDOR IS ALLOWED TO CONTROL THE DEFENSE OF ANY CLAIM HEREUNDER, INCLUDING SETTLEMENT OF SUCH CLAIM, IN LITIGATION OR OTHERWISE, VENDOR'S SELECTION OF LEGAL COUNSEL AND ANY SETTLEMENT REQUIRING ANY ADMISSION OF LIABILITY BY EISD, IMPOSING ANY PECUNIARY OR EQUITABLE OBLIGATION ON EISD, OR ADVERSELY AFFECTING ANY RIGHTS OF EISD UNDER THIS AGREEMENT OR APPLICABLE LAW SHALL BE SUBJECT TO EISD'S PRIOR WRITTEN CONSENT.

NOTHING IN THIS AGREEMENT SHALL BE CONSTRUED AS LIMITING VENDOR'S OBLIGATIONS UNDER THIS SECTION. THE PARTIES AGREE THAT, WITH RESPECT TO ANY LEGAL LIMITATIONS NOW OR HEREAFTER IN EFFECT AND AFFECTING THE VALIDITY OR ENFORCEABILITY OF VENDOR'S OBLIGATIONS HEREUNDER, SUCH LEGAL LIMITATIONS ARE MADE A PART OF VENDOR'S OBLIGATIONS HEREUNDER TO THE MINIMUM EXTENT NECESSARY TO BRING THE PROVISION INTO CONFORMITY

WITH THE REQUIREMENTS OF SUCH LIMITATIONS, AND AS SO MODIFIED, VENDOR'S OBLIGATIONS HEREUNDER SHALL CONTINUE IN FULL FORCE AND EFFECT.

NOTHING IN THIS AGREEMENT SHALL BE CONSTRUED TO CREATE A CLAIM OR CAUSE OF ACTION AGAINST EISD FOR WHICH IT IS NOT OTHERWISE LIABLE, OR TO REQUIRE EISD TO INDEMNIFY VENDOR, ITS EMPLOYEES, AGENTS, AFFILIATES, OR ANY OTHER PARTY IN ANY CAPACITY OR OTHERWISE CREATE AN IMPERMISSIBLE INDEMNIFICATION OBLIGATION OR DEFICIENCY DEBT OF EISD.

14. **Confidential Information:** A party may provide confidential or proprietary information to the other party in connection with this Agreement that: (1) is marked as being confidential or proprietary; (2) if delivered in oral form, is summarized in writing within ten (10) EISD business days and identified as being confidential or proprietary; (3) should be reasonably understood by the receiving party to be confidential or proprietary in light of the type or nature of the information or circumstances associated with the disclosure of the information; or (4) is made confidential by law (collectively, "Confidential Information").

It is expressly understood and agreed by the parties that Confidential Information includes the Software and Documentation, any District Data (as defined in the DPA), and any EISD and third-party intellectual property, EISD system(s), and other information processed or stored on computers or other electronic media by EISD or on EISD's behalf, provided to Vendor for such processing or storage, or otherwise provided or made available to Vendor by EISD, its employees, students, parents, contractors, agents, and affiliates in connection with this Agreement or the Services.

Except to the extent that a more stringent requirement applies to District Data pursuant to the DPA or applicable law, which requirement shall control in all cases, the receiving party shall: (i) hold Confidential Information in strict confidence, using commercially reasonable measures to maintain the confidentiality and security of Confidential Information; (ii) except as previously authorized in writing by the disclosing party, not publish or disclose Confidential Information to anyone other than the receiving party's employees on a need-to-know basis, provided that such employees are bound, in writing or through reasonable employment contracts and/or policies of the receiving party, to confidentiality obligations no less restrictive than those set forth herein; and (iii) use Confidential Information solely for the purpose of providing Services to EISD under this Agreement for the benefit of EISD and its students and for no other purpose.

15. **Injunctive Relief:** The parties agree that a violation, or threatened violation, of Section 14 (Confidential Information) shall be deemed to cause irreparable harm, for which monetary damages would not provide adequate compensation, that justifies immediate injunctive relief against such breach or threatened breach without proving actual damage or posting a bond or other security and, without limiting any rights, remedies, or defenses available to the parties, may result in termination of this Agreement for cause.
16. **Compelled Disclosure:** Nothing in this Agreement shall be construed as prohibiting EISD from disclosing any information related to or in connection with this Agreement or the Services in accordance with applicable law, including court order, subpoena, and the Texas Public Information Act, or as imposing any liability on EISD in connection with any such disclosure. In the event that EISD is required to disclose information in response to a request under the Texas Public Information Act or other applicable law, EISD's compliance with the requirements of the Texas Public Information Act or such other applicable law, which may or may not require notice to Vendor, shall be deemed sufficient to satisfy any obligations of EISD regarding confidential or proprietary information under this Agreement, and Vendor hereby waives any claim against and releases from liability EISD, its officers, employees, agents, and attorneys with respect to any such disclosure.
17. **Protected Health Information:** If EISD determines that the Vendor, its employees, subcontractors, or agents will access, maintain, use, or disclose "protected health information" subject to the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub.L. 111-5) ("HITECH"), and/or the Texas Medical Records Privacy Act, Tex. Health & Safety Code

Ann.§ 181.001 et seq. ("TMRPA"), in addition to and as part of the terms and conditions of this Agreement, the parties agree to enter into a Business Associate Agreement, in form and substance reasonably agreeable to both parties, providing for the privacy and security of such protected health information as required by HIPAA, HITECH, and the TMRPA, as such laws may be amended from time to time by the authorities having jurisdiction thereof.

18. **Subcontractors:** If Vendor is permitted to use subcontractors in the performance of any part of this Agreement, Vendor shall ensure that each subcontractor complies with all provisions of this Agreement, and Vendor shall be fully responsible to EISD for any and all acts and omissions of the subcontractor(s) just as Vendor is responsible for Vendor's own acts and omissions. Nothing in this Agreement shall create for the benefit of any such subcontractor any contractual relationship between EISD and any such subcontractor, nor shall it create any obligation on the part of EISD to pay or to see to the payment of any monies due any such subcontractor except as may otherwise be required by law.
19. **Termination for Convenience:** EISD may terminate this Agreement for convenience, in whole or in part, at any time, without penalty, liability, or further obligation, upon providing at least thirty (30) days advance written notice to Vendor. In the event of such termination, Vendor will be paid for all Services actually provided and duly accepted by EISD up to the effective date of termination, less any compensation already paid. For the avoidance of doubt, in no event will any Services be deemed to have been provided or accepted for any period beyond the then-current year of the Term.
20. **Termination for Cause:** A party will be in default of this Agreement if such party fails to comply with any obligation in this Agreement and such failure continues for ten (10) EISD business days after receiving written notice of default from the non-defaulting party. In the event of default, the non-defaulting party, upon written notice to the defaulting party, may terminate this Agreement for cause, without penalty, liability, or further obligation, as of the date specified in the notice, and may seek other relief as provided by law. In the event of termination by EISD for cause during the Term of this Agreement, without limiting any rights or remedies of EISD under this Agreement or applicable law, EISD shall be entitled to a refund of an equitable portion of any fees, including, but not limited to, any license, subscription, hosting, and maintenance fees, paid by EISD for the affected Services.
21. **SLA Material Breach and Termination:** For purposes of this Section, an "Interruption in Services" shall mean that the Software has stopped working or has been severely impacted such that most functions or one or more critical business functions are unusable by EISD for 8 hours or more as a result of failure of Vendor-provided facilities, equipment, personnel, or other services. In the event of 2 or more Interruptions in Services during any one-month period or 3 or more Interruptions in Services during any six-month period, EISD may terminate this Agreement for cause in accordance with Section 20, above.
22. **Non-Appropriation of Funds:** The parties agree that this Agreement is a commitment of EISD's current revenue only. Notwithstanding any contrary provision of this Agreement, any payment obligation(s) of EISD created by this Agreement shall be conditioned upon the availability of funds that are duly appropriated and allocated for such purpose. If such funds are not available, as determined by EISD in its sole discretion, EISD shall have the right to terminate this Agreement, without default, penalty, or further obligation or liability to Vendor, effective at the end of the period for which such funds are available. In the event this provision is exercised, EISD shall provide written notice of non-appropriation, specifying the effective date of termination, to Vendor as soon as reasonably practicable.
23. **Transition Obligations:** Upon termination of this Agreement, the following shall apply:
 - a. The parties shall reasonably, and in good faith, negotiate and agree, in writing, upon a transition plan ("Transition Plan") providing, at a minimum, for:
 - i. A final transition term agreeable to both parties, but not less than the time reasonably required by EISD to procure and implement replacement services ("Transition Period");
 - ii. Vendor's provision to EISD of reasonable assistance in transitioning to another vendor, as deemed necessary by EISD, including, but not limited to, continued access to and use of the Services as set forth under this Agreement and any transition-related services

offered by Vendor, (collectively, "Transition Services"), subject to EISD's payment of the Transition Fees (as defined below);

- iii. Reasonable pro-rated fees for the Transition Services ("Transition Fees"), provided that the Transition Fees shall apply only to the extent that the Transition Services exceed the scope of Services already provided for under this Agreement and that any applicable Transition Fees shall not exceed the fees agreed upon by the parties in Exhibit A or offered by Vendor in Vendor's proposal submitted in response to [Applicable District RFP Document], prorated for EISD's actual use of the Transition Services during the Transition Period; and
- iv. The date upon which EISD's access to and use of the Services will terminate, subject to any reduction or extension of the Transition Period reasonably agreed upon by the parties in writing.

24. **Independent Contractor:** EISD and Vendor hereby agree that, in performing the Services, Vendor will be deemed an independent contractor and not EISD's employee or agent. This Agreement will not be construed to create any partnership, joint venture, or other similar relationship between EISD and Vendor or EISD and any of Vendor's employees or agents. As an independent contractor, Vendor will be solely responsible for determining the means and methods for performing the Services and shall furnish all tools, materials, transportation, and personal incidentals necessary in the performance of the Services. Vendor agrees that EISD has no responsibility for any conduct of any of Vendor's employees, agents, representatives, contractors, or subcontractors.
25. **Use of EISD Name or Logos:** Vendor shall not use EISD's name, logo, any phrase associated with EISD, or other likeness without prior written permission from EISD's Board of Trustees, Superintendent of Schools, or their designee.
26. **Non-Solicitation:** Neither party shall knowingly solicit any of the other party's employees involved in this Agreement, during the Term of this Agreement and for a period of one (1) year from the termination thereof, without the express written consent of the other party. Nothing in this Agreement shall be construed as restricting the right of either party to solicit or recruit generally in the media.
27. **Time is of the Essence:** Time is of the essence in the performance of this Agreement.
28. **Notices:** Any notice required or permitted by this Agreement shall be in writing and addressed to the party at the address set forth below, or such other address as is subsequently specified by written notice in the manner provided herein. Notices shall be effective as of: (i) the date delivered by hand, (ii) three (3) EISD business days after such notice shall have been deposited with a national courier service or Registered/Certified U.S. Mail, postage prepaid, return receipt requested, with a courtesy copy of such notice provided by email on the date of such deposit; or (iii) if not provided in accordance with (i) or (ii) above, the date such notice is actually received.

To EISD:

To Vendor:

29. **Compliance with Law:** Vendor agrees to observe and abide by all applicable state, federal, and local laws, as currently written and as may be amended from time to time by the authorities having jurisdiction over such matters, in the performance of this Agreement.
30. **Insurance Requirements:** Vendor shall make adjustments to insurance coverages and limits as reasonably prudent, based upon changes in statutory laws, court decisions, or potential increase in exposure to loss, in order for Vendor to maintain commercially reasonable, industry standard insurance coverages and limits

sufficient to cover any Vendor risks, liabilities, or other obligations that may arise under this Agreement. Noncompliance or misrepresentation regarding this Section may be grounds for immediate termination of this Agreement for cause.

31. **Records Retention and Audit by EISD:** Vendor shall maintain its records and accounts in a manner that shall assure a full accounting for all goods and services provided by Vendor to EISD under this Agreement. These records and accounts shall be retained by Vendor and made available for audit by EISD for a period of not less than 10 years from the date of completion of the Services or the date of EISD's final payment in connection with this Agreement, whichever is later. If an audit has been announced, Vendor shall retain its records and accounts until such audit has been completed. When federal funds are expended by EISD pursuant to this Agreement, Vendor certifies that it will comply with the record retention requirements detailed in 2 CFR § 200.333. Vendor further certifies that Vendor will retain all records as required by 2 CFR § 200.333 for a period of three years after grantees or subgrantees submit final expenditure reports or quarterly or annual financial reports, as applicable, and all other pending matters are closed.

Upon written notice from EISD, Vendor shall permit EISD's internal and external auditors, the Texas Education Agency, the Comptroller General of the United States, or any of their duly authorized representatives (collectively, "Auditor") to conduct audits or investigations in connection with this Agreement. Vendor agrees to cooperate with the Auditor conducting such audits or investigations and to provide the Auditor access to or copies of any books, documents, papers, and records of Vendor which are directly pertinent to this Agreement, for the purpose of making audit, examination, excerpts, and transcriptions.

32. **Software Audits:** Notwithstanding any contrary provision of this Agreement, during the Term of this Agreement, Vendor may, at Vendor's sole cost and expense, conduct commercially reasonable audits of EISD's use of the Software no more than once per calendar year. Vendor shall provide EISD not less than ten (10) EISD business days' prior written notice of any such audit. EISD will reasonably cooperate with such audit, including providing access, at EISD's facilities, during EISD's regular business hours, to EISD's books, computers, records, or other information to the extent directly pertinent to EISD's use of the Software and as reasonably necessary to determine EISD's compliance with this Agreement; provided that EISD shall be entitled to reasonably redact any confidential or proprietary information contained therein. Any audit conducted hereunder shall not unreasonably interfere with EISD's business activities. If Vendor discovers any unauthorized use, reproduction, or distribution of the Software by EISD, subject to any necessary approvals by EISD's administration and Board of Trustees, EISD in its sole discretion, may elect to (1) pay to Vendor the reasonable, actual cost of such unauthorized use, reproduction, or distribution, based on the fees set forth in Exhibit A and Vendor's proposal submitted in response to [*Applicable District RFP Document*], which payment shall be Vendor's sole and exclusive remedy in connection with any such unauthorized use, reproduction, or distribution; or (2) dispute Vendor's determination that any such unauthorized use, reproduction, or distribution has occurred and assert any defense available at law, in equity, or otherwise.

33. **Severability:** If any provision of this Agreement is found to be invalid or unenforceable, the remaining provisions of this Agreement shall be construed as if such invalid or unenforceable provision had never been contained herein.

34. **Contract Interpretation:** The parties acknowledge that this Agreement is the result of substantial negotiations between the parties and agree that nothing in this Agreement shall be construed or interpreted against either party because such party or its legal counsel drafted the Agreement.

35. **Force Majeure:** Neither party's delay or failure to perform any obligation under this Agreement shall be deemed a breach of this Agreement to the extent that such delay or failure is due to an act of God, storm, flood, washout, governmental order, regulation, or other action, disease, including epidemic and pandemic, fire, war, insurrection, riot, act of the public enemy or terrorist act strike, civil disturbance, or any other cause beyond the reasonable control of the party claiming force majeure and which by the exercise of due diligence such party is unable to prevent or overcome; provided that force majeure shall only exist during the continuance of such cause and no longer and that the party claiming force majeure shall attempt to

remedy such cause with reasonable dispatch and shall resume performance immediately after the obstacles to performance caused by the force majeure event have been removed. Notwithstanding any other provision of this Agreement, in the event that Vendor's performance of its obligations under this Agreement is delayed or stopped by a force majeure event for thirty (30) days or more, EISD shall have the right to terminate this Agreement without penalty or further obligation upon written notice to Vendor. This Section shall not be interpreted as to limit or otherwise modify any of the parties' contractual, legal, or equitable rights.

36. **Governing Law/Venue:** This Agreement shall be governed by the laws of the State of Texas without regard to conflicts of law principles. Mandatory and exclusive venue for any dispute arising out of this Agreement or the Services shall be a court of competent jurisdiction in Travis County, Texas, and the parties hereby submit to the jurisdiction of said courts. Nothing in this Agreement shall be construed as requiring EISD to subject any dispute arising out of this Agreement to mediation or arbitration.
37. **Amendment:** This Agreement may be modified or amended only in writing, properly executed by both Vendor and EISD, including any necessary approvals by EISD's administration and Board of Trustees, and attached hereto.
38. **Waiver:** A party may waive a provision or requirement of this Agreement only in writing, properly executed by such party. A party's waiver of a provision or requirement of this Agreement shall not be effective as to any other provision or requirement of this Agreement or any subsequent breach of the same provision or requirement. Nothing in this Agreement shall be construed as a waiver or relinquishment of any governmental immunities or defenses on behalf of EISD, its trustees, officers, employees, or agents as a result of the execution of this Agreement or performance of the functions or obligations described herein.
39. **Non-Exclusivity:** Nothing in this Agreement shall be construed as limiting any rights or remedies of EISD under this Agreement or applicable law.
40. **Assignment:** No assignment of this Agreement or of any duty or obligation or performance hereunder, shall be made in whole or in part by either party without the prior written consent of the other party. Any assignee of Vendor shall satisfy the standard minimum qualifications required to do business with EISD, including EISD's insurance requirements and any required Vendor disclosures and certifications.
41. **Captions:** The captions herein are for convenience and identification purposes only, are not an integral part hereof, and are not to be considered in the interpretation of any part hereof.
42. **Survival:** The following provisions shall survive termination of this Agreement: Sections 1, 6-9, 11-16, 18-20, 22-26, 28, 29, 30-42, 45-47; and (2) any other provision of this Agreement that must survive to fulfill its essential purpose.
43. **Certification of Non-Indebtedness to EISD:** Pursuant to Section 44.044, Texas Education Code, by resolution, EISD may establish regulations permitting it to refuse to enter into a contract with a person indebted to it. A person, under this Section, includes an individual, sole proprietorship, corporation, nonprofit corporation, partnership, joint venture, limited liability company, and any other entity that proposes or otherwise seeks to enter into a contract or other transaction with EISD requiring approval by its Board of Trustees. By executing this Agreement, Vendor certifies that it is not indebted to EISD.
44. **HB 793/SB 252 Certifications:** Vendor certifies that it is not a company identified on the Texas Comptroller's list of companies known to have contracts with, or provide supplies or services to, a foreign organization designated as a Foreign Terrorist Organization by the U.S. Secretary of State under federal law. If (a) Vendor is not a sole proprietorship; (b) Vendor has ten (10) or more full-time employees; and (b) this Agreement has a value of \$100,000 or more, the following certification shall apply; otherwise, this certification is not required. Pursuant to Chapter 2270 of the Texas Government Code, the Vendor hereby certifies and verifies that neither the Vendor, nor any affiliate, subsidiary, or parent company of the Vendor, if any (the "Vendor Companies"), boycotts Israel, and the Vendor agrees that the Vendor and Vendor Companies will not boycott Israel during the Term of this Agreement. For purposes of this

Agreement, the term “boycott” shall mean and include refusing to deal with, terminating business activities with, or otherwise taking any action that is intended to penalize, inflict economic harm on, or limit commercial relations with Israel, or with a person or entity doing business in Israel or in an Israeli-controlled territory, but does not include an action made for ordinary business purposes.

45. **SB 943 Certification:** If Vendor is not a governmental body and (a) this Agreement has a stated expenditure of at least \$1 million in public funds for the purchase of goods or services by EISD; or (b) this Agreement results in the expenditure of at least \$1 million in public funds for the purchase of goods or services by EISD in a fiscal year of EISD, the following certification shall apply; otherwise, this certification is not required. As required by Tex. Gov’t Code § 552.374(b), the following statement is included in the RFP and the Agreement (unless the Agreement is (1) related to the purchase or underwriting of a public security; (2) is or may be used as collateral on a loan; or (3) proceeds from which are used to pay debt service of a public security of loan): “The requirements of Subchapter J, Chapter 552, Government Code, may apply to this RFP and Agreement and the contractor or vendor agrees that the contract can be terminated if the contractor or vendor knowingly or intentionally fails to comply with a requirement of that subchapter.” Pursuant to Subchapter J, Chapter 552, Texas Government Code, the Vendor hereby certifies and agrees to (1) preserve all contracting information related to this Agreement as provided by the records retention requirements applicable to EISD for the duration of the Agreement; (2) promptly provide to EISD any contracting information related to the Agreement that is in the custody or possession of the Vendor on request of EISD; and (3) on completion of the Agreement, either (a) provide at no cost to EISD all contracting information related to the Agreement that is in the custody or possession of Vendor, or (b) preserve the contracting information related to the Agreement as provided by the records retention requirements applicable to EISD.
46. **Limitations:** THE PARTIES ARE AWARE THAT THERE ARE CONSTITUTIONAL AND STATUTORY LIMITATIONS ON THE AUTHORITY OF EISD (A PUBLIC SCHOOL) TO ENTER INTO CERTAIN TERMS AND CONDITIONS OF THIS AGREEMENT, INCLUDING, BUT NOT LIMITED TO, THOSE TERMS AND CONDITIONS RELATING TO LIENS ON EISD’S PROPERTY; DISCLAIMERS AND LIMITATIONS OF WARRANTIES; DISCLAIMERS AND LIMITATIONS OF LIABILITY FOR DAMAGES; WAIVERS, DISCLAIMERS AND LIMITATIONS OF LEGAL RIGHTS, REMEDIES, REQUIREMENTS AND PROCESSES; LIMITATIONS OF PERIODS TO BRING LEGAL ACTION; GRANTING CONTROL OF LITIGATION OR SETTLEMENT TO ANOTHER PARTY; LIABILITY FOR ACTS OR OMISSIONS OF THIRD PARTIES; PAYMENT OF ATTORNEYS’ FEES; DISPUTE RESOLUTION; INDEMNITIES; AND CONFIDENTIALITY (COLLECTIVELY, THE “LIMITATIONS”), AND TERMS AND CONDITIONS RELATED TO THE LIMITATIONS WILL NOT BE BINDING ON EISD EXCEPT TO THE EXTENT AUTHORIZED BY THE LAWS AND CONSTITUTION OF THE STATE OF TEXAS.
47. **Entire Agreement:** Notwithstanding any contrary provision of any Agreement Document, this Agreement constitutes the entire agreement between the parties regarding the Services, and supersedes all prior contracts, agreements, representations, and understandings made by the parties relating to such subject matter. EISD expressly rejects any other agreements, terms, conditions, or policies, including, any terms of use, licensing agreements, privacy policies, or other agreements or understandings, that may be incorporated by reference in Exhibit D, pre-published on any Vendor or third-party websites, order acknowledgments, invoices, or forms, or otherwise provided by Vendor or any third party in connection with the Services, whether electronic, click-through, verbal, or in writing, regardless of any agreement thereto by EISD employees or agents, and any such agreements shall be null, void, and without effect unless properly executed by EISD and attached to this Agreement as an Agreement Document. Notwithstanding any contrary provision therein, no subsequent revision or modification to any Vendor Agreement Document shall be binding upon EISD unless properly executed by EISD and attached hereto.

[SIGNATURE PAGE FOLLOWS]

IN WITNESS WHEREOF, the parties have executed this Agreement effective as of _____, 20__.

VENDOR: _____

BY: _____
Printed Name: _____
Title: _____
Date: _____

EANES INDEPENDENT SCHOOL DISTRICT

BY: _____
Printed Name: _____
Title: _____
Date: _____

DATA PROTECTION ADDENDUM (“DPA”)

This DATA PROTECTION ADDENDUM (“DPA”) is entered into by and between _____ (“Vendor”) and Eanes Independent School District (“District”) (collectively, the “Parties” and each individually, a “Party”), to address Vendor’s access to, and use, maintenance, and disclosure of, District Data (as defined below). This DPA is hereby made part of the EISD Software Agreement between the Parties dated [INSERT EFFECTIVE DATE OF AGREEMENT] (the “Agreement”), as of the effective date set forth in the Agreement (the “Effective Date”), as a condition to Vendor’s access to District Data in connection with the Agreement. In the event of any conflicts or inconsistencies between or among this DPA, the Agreement, and/or applicable law, the Parties agree that the requirement that affords the most protection to District Data will supersede and prevail.

1. Definitions

- A. “Contracted Third Party” means a subcontractor or other third party with whom the Vendor has contracted to provide Services for or on behalf of the Vendor for a School Purpose under the Agreement.
- B. “District Data” means all information, including, but not limited to, business, administrative, financial, student, and personnel information, and work product or other intellectual property that is: (1) created by the District, its employees, contractors, agents, affiliates, students, parents, and users, or provided or otherwise made available to Vendor, its employees, agents, or subcontractors by the District, its employees, contractors, agents, affiliates, students, parents, and users through the Services or otherwise in connection with the Agreement, or (2) gathered by Vendor, its employees, agents, or subcontractors through the Services or other means (e.g., Vendor technology) in connection with the Agreement. District Data includes, but is not limited to:
 - 1. Personal identifiers such as name, address, phone number, date of birth, Social Security number, identification number, persistent unique identifiers, and the like;
 - 2. Any personal information protected by law, including, but not limited to:
 - a. “personally identifiable information” and student “education records” as those terms are defined under the Family Educational Rights and Privacy Act, 20 USC 1232g, as amended (“FERPA”);
 - b. “personal information” as that term is defined in the Children’s Online Privacy Protection Act of 1998 (“COPPA”);
 - c. “personal information” as that term is defined in the Protection of Pupil Rights Amendment (“PPRA”);
 - d. “personally identifiable information” as that term is defined in the Individuals with Disabilities Education Act, as amended (“IDEA”);
 - e. “covered information” as defined under Chapter 32, Subchapter D, Texas Education Code;
 - f. “personal identifying information” and “sensitive personal information” as defined under the Texas Identity Theft Enforcement and Protection Act (Chapter 521, Texas Business and Commerce Code);
 - g. nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809 (“GLB”);
 - h. credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards (“PCI-DSS”);
 - 3. Other financial account numbers, access codes, driver’s license numbers;
 - 4. State or federal identification numbers such as passport, visa or state identity card numbers;
 - 5. Information that identifies an individual and relates to the physical or mental health or condition of the individual, the provision of health care to the individual, or payment for the provision of health care to the individual; and
 - 6. The types or categories of information expressly listed in Exhibit A attached hereto, if any.
- C. “Mining District Data” means to search through, access, manipulate, or extract District Data for a purpose other than providing Services to the District for a School Purpose under the Agreement.
- D. “School Purpose” means a purpose that is directed by or customarily takes place at the direction of a school district, school campus, or teacher or assists in the administration of school activities, including instruction

in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents, or is otherwise for the use and benefit of the school.

- E. "Securely Destroy" means taking commercially reasonable actions that render data written on physical or electronic media unrecoverable, including, but not limited to, actions that meet or exceed those sections of the National Institute of Standards and Technology (NIST) SP 800-88 guidelines relevant to data categorized as high security (provided that, in accordance with NIST 800-88r1 guidance, Vendor shall comply with the level "purge" with a Cryptographic Erase (*i.e.*, not a simple delete/erase that leaves the previous contents available until overwritten through normal use) while the media is still in operation and under the actual or constructive possession and control of Vendor and "destroy" only when the media has reached end of life (EOL) and/or will no longer be under the actual or constructive possession and control of Vendor), or the DoD 5220.22-M (3 pass) data sanitization method, as applicable.
- F. "Security Incident" means an event in which District Data is exposed to unauthorized disclosure, access, alteration, or use, or circumstances that are reasonably expected to have exposed District Data to unauthorized disclosure, access, alteration, or use.
- G. "Services" means the products and/or services provided to the District in connection with the Agreement.
- H. "Targeted Advertising" means presenting an advertisement to a student in which the advertisement is selected for the student based on information obtained or inferred over time from the student's online behavior, usage of applications, or covered information. The term does not include advertising to a student at an online location based on the student's visit to that location at that time, or in response to the student's request for information or feedback, without the retention of the student's online activities or requests over time for the purpose of targeting subsequent advertisements.

Technical terms not defined herein that have a well-known technical or trade meaning, shall be held to have such recognized meaning.

2. Rights In and To District Data

Vendor agrees that, as between the District and Vendor, District Data is and shall remain the sole and exclusive property of the District. The District hereby authorizes the Vendor to access, maintain, use, and disclose District Data, subject to the terms and conditions of the Agreement, this DPA, and applicable law, solely as reasonably necessary to provide Services to the District for a School Purpose under the Agreement. Vendor has no rights, implied or otherwise, to District Data, except as expressly stated in this DPA.

3. Vendor's Use and Disclosure of District Data

- a. Vendor shall access, maintain, use, and disclose District Data, subject to the terms and conditions of the Agreement, this DPA, and applicable law, solely as reasonably necessary to provide Services to the District for a School Purpose under the Agreement.
- b. Vendor is prohibited from Mining District Data unless such activity is permitted by law and expressly authorized by the District in advance in writing.
- c. Except as expressly permitted under this DPA, Vendor will not disclose or allow the disclosure of District Data, including any goods, products, materials, documents, reports, writings, video images, photographs, papers, or software or computer images of any nature prepared by Vendor, its employees, agents, or subcontractors that incorporate District Data, to any other person or entity.
- d. To the extent permitted by law, and solely as reasonably necessary to provide Services to the District for a School Purpose under the Agreement, Vendor may provide access to, export, transfer, or otherwise disclose District Data to Vendor's employees and Contracted Third Parties; provided, however, that: (1) prior to any such disclosure, the employee or Contracted Third Party receiving District Data has agreed in writing to comply with data protection obligations substantially similar to, and in no event less restrictive than, those applicable to Vendor under the Agreement, this DPA, and applicable law; (2) if the party receiving District Data is a Contracted Third Party, Vendor's contract with any such Contracted Third Party: (i) prohibits the Contracted Third Party from using District Data for any purpose other than providing Services to the District for a School Purpose under the Agreement, and (ii) requires the Contracted Third Party to implement and maintain reasonable procedures and practices designed to prevent disclosure of District Data; and (3) the employee or Contracted Third Party shall not further disclose District Data.

- e. Vendor shall, prior to disclosing District Data, ensure that any Vendor employees, agents, and subcontractors who will have access to District Data have, prior to any such access, undergone appropriate, commercially reasonable background screening and other screening as required by law, and that any such employees, agents, and subcontractors possess all necessary qualifications and have read, understood, and received appropriate instruction as to how to comply with the requirements of the Agreement, this DPA, and applicable law.
- f. If, in connection with the Agreement, the Vendor must create, obtain, transmit, use, maintain, process, or dispose of personal information that is protected by law or financial or business data that has been identified to the Vendor as having the potential to affect the accuracy of the District's financial statements, Vendor shall perform the following background checks on all employees, subcontractors, and agents are reasonably expected to have access to such data in accordance with the Fair Credit Reporting Act: Social Security Number trace; seven (7) year felony and misdemeanor criminal records check of federal, state, or local records (as applicable) for job related crimes; Office of Foreign Assets Control List (OFAC) check; Bureau of Industry and Security List (BIS) check; and Office of Defense Trade Controls Debarred Persons List (DDTC).
- g. Vendor will not otherwise access, maintain, or use District Data or share District Data with or disclose it to any third party without the prior written consent of the District, except as required by law in accordance with Section 9 of this DPA.

4. FERPA Acknowledgements

- a. Vendor acknowledges that, for purposes of the Agreement, it will be designated a "school official" with "legitimate educational interests" in "personally identifiable information" and student "education records", as those terms have been defined under FERPA and its implementing regulations, and Vendor agrees to abide by the FERPA limitations and requirements imposed upon school officials.
- b. The District and Vendor expressly agree that: (1) the services/functions to be provided by Vendor are services/functions for which the District would otherwise use its own employees; (2) Vendor has been determined to meet the criteria set forth in the District's annual notification of FERPA rights for being a school official with legitimate educational interests in the "personally identifiable information" and student "education records" disclosed to Vendor for purposes of the Agreement; (3) Vendor is under the District's direct control with respect to its access to, and maintenance, use, and disclosure of, "personally identifiable information" and student "education records"; and (4) unless Vendor has specific written authorization from the District to do so and it is otherwise permitted by FERPA, Vendor will access, maintain, use, and disclose "personally identifiable information" and student "education records" only for the purpose for which the disclosure was made and will not re-disclose "personally identifiable information" and student "education records" to other parties.
- c. To the extent that students or parents/guardians may be required to accept or are otherwise made subject to any separate terms of use, privacy policies, or other agreement(s) (e.g., click-through terms and conditions or other agreements) in connection with the Services or the Agreement, Vendor shall ensure that no such agreement (including any Contracted Third Party's agreement) requires the student or parent/guardian to waive any rights or other protections to which he/she may be entitled under FERPA. Any provision in such agreement(s) to the contrary shall be null, void, and without effect and this DPA shall apply.

5. Data Security and Confidentiality

- a. District Data, whether electronic format or hard copy, must be secured and protected at all times to avoid unauthorized access. Vendor will store and process District Data in accordance with commercial best practices, including, but not limited to, implementing and maintaining appropriate administrative, physical, and technical safeguards and other security procedures and practices designed to preserve the confidentiality, integrity and availability of District Data and protect such data from unauthorized access, deletion, disclosure, modification, interception, diversion, and use. Such measures will be no less protective than those used to secure Vendor's own data of a similar type, and in no event less than commercially reasonable in view of the type and nature of the data involved. These requirements will be extended by contract to all subcontractors and agents used by Vendor.

- b. Vendor will use industry-standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing the Services under the Agreement and accessing, maintaining, using, and disclosing District Data in connection therewith.
- c. Without limiting the foregoing, Vendor agrees that Vendor, its subcontractors and agents (including any data center), as applicable, shall meet or exceed the following standards and requirements in maintaining the security and confidentiality of District Data in connection with the Agreement:
 - i. PCI-DSS v3.2 requirements;
 - ii. TIA 942 Class 4 Data Center Standards or a substantially similar standard;
 - iii. All electronic District Data will be encrypted in transmission using Transmission Layer Security (TLS) v1.2 or greater (including via web interface or equivalent); and
 - iv. All electronic District Data stored on a mobile device, laptop, desktop or any other device that does not meet the requirements of (i) or (ii) above will be encrypted at no less than AES 128-bit level encryption.
- d. Vendor shall, upon request, provide the District with a reasonably detailed written summary of the procedures Vendor, its subcontractors and agents use to maintain and transmit District Data.
- e. District Data shall not be stored outside the United States without the District's prior written consent.
- f. Vendor will take commercially reasonable measures, including, but not limited to, audit trails, to protect District Data from deterioration or degradation of data quality and authenticity.
- g. Vendor will regularly back up District Data in a commercially reasonable manner and retain any such backups for a minimum of 12 months.

6. Security Incidents

- a. Response. Upon becoming aware of a Security Incident, Vendor will immediately, and within the time reasonably necessary for the Parties to comply with applicable legal requirements, (1) notify the District's Superintendent of Schools to begin remediation of compromised data, (2) fully investigate the incident, and (3) cooperate as reasonably requested with the District's investigation of and response to the incident. Except as otherwise required by law, and without affecting Vendor's obligations under Section 6(b), below, the District will, in its sole discretion, provide or, alternatively, direct Vendor to provide any breach notification required by laws applicable to District Data in connection with the Security Incident, and Vendor will not provide notice of the incident directly to individuals whose personal information was involved, regulatory agencies, or other entities, without prior written permission from the District.
- b. TO THE FULLEST EXTENT PERMITTED BY LAW, AND IN ADDITION TO ANY OTHER RIGHTS OR REMEDIES OF THE DISTRICT UNDER CONTRACT, LAW, OR EQUITY, TO THE EXTENT THAT ANY SECURITY INCIDENT ARISES OR RESULTS FROM VENDOR'S, ITS EMPLOYEE'S, SUBCONTRACTOR'S, OR AGENT'S FAILURE TO COMPLY WITH ANY REQUIREMENT OF THE AGREEMENT, THIS DPA, OR APPLICABLE LAW, THE VENDOR HEREBY AGREES TO DEFEND, INDEMNIFY AND HOLD THE DISTRICT, ITS TRUSTEES, AGENTS, EMPLOYEES, CONTRACTORS, AND VOLUNTEERS HARMLESS FROM AND AGAINST ANY AND ALL CLAIMS, DEMANDS, CAUSES OF ACTION, LIABILITY, FINES, PENALTIES, COSTS, DAMAGES, LOSSES, JUDGMENTS, AND EXPENSES (INCLUDING ATTORNEYS' FEES), INCLUDING, BUT NOT LIMITED TO: (1) ALL COSTS INCURRED BY THE DISTRICT IN CONNECTION WITH THE INVESTIGATION AND REMEDIATION OF THE SECURITY INCIDENT; (2) THE COST OF PROVIDING NOTIFICATION TO INDIVIDUALS OR ENTITIES WHOSE INFORMATION WAS COMPROMISED AND TO REGULATORY AGENCIES OR OTHER ENTITIES AS REQUIRED BY LAW OR CONTRACT; (3) PROVIDING ONE YEAR OF CREDIT MONITORING TO AFFECTED INDIVIDUALS IF PERSONAL INFORMATION EXPOSED DURING THE INCIDENT COULD BE USED TO COMMIT IDENTITY THEFT; (4) ALL CRISIS MANAGEMENT, REGULATORY RESPONSE, AND OTHER PRIVACY LIABILITY COSTS; AND (5) THE PAYMENT OF LEGAL FEES, AUDIT COSTS, FINES, CIVIL PENALTIES, AND OTHER FEES IMPOSED AGAINST THE DISTRICT IN CONNECTION WITH THE SECURITY INCIDENT.

7. Response to Legal Orders, Demands or Requests for Data

- a. Except as expressly prohibited by law, Vendor will:

- i. Immediately, and before disclosing any District Data, notify the District, in writing, of any subpoenas, warrants, or other orders, demands or requests received by Vendor, its employees, subcontractors or agents seeking District Data;
 - ii. Reasonably consult with the District regarding Vendor's response, which may include, but is not limited to, directing the requestor to seek the information directly from the District, as appropriate;
 - iii. Cooperate with the District's reasonable requests in connection with efforts by the District to intervene and quash or modify the order, demand, or request; and
 - iv. Upon the District's request, provide the District with a copy of its response.
- b. If the District receives a subpoena, warrant, or other order, demand, or request (including, but not limited to, a request for information pursuant to the Texas Public Information Act, FERPA, or similar law) seeking District Data in the Vendor's, its employees', subcontractors', or agents' actual or constructive possession, custody, or control, the District will provide information regarding the request to Vendor and provide a deadline by which the Vendor must supply the District with records or information required for the District to timely respond to the request. Vendor will ensure that all requested records and information are supplied to the District by the deadline provided by the District and will reasonably cooperate with the District's other requests in connection with the District's response.

8. Data Transfer/Destruction

- a. Upon termination of the Agreement, or as otherwise requested by the District in writing, Vendor shall ensure that all District Data in Vendor's, its employees', subcontractors', and agents' actual or constructive possession, custody, or control is transferred to the District (or a third party designated by the District) as reasonably directed by the District.
- b. Transfer of District Data to the District (or a third party designated by the District) shall occur within a reasonable period of time following termination of the Agreement or the District's written request. Vendor will use commercially reasonable efforts to ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of the District or its designated transferee, and to the extent reasonably technologically feasible, that the District will have access to District Data during the transition.
- c. If the District requests destruction of any District Data at any time, not later than sixty (60) days after the date of the District's request, Vendor shall Securely Destroy all such District Data in its actual or constructive possession, custody, or control and ensure that all District Data in the actual or constructive possession, custody, or control of Vendor's employees, subcontractors, and agents is Securely Destroyed. Notwithstanding the foregoing, unless otherwise directed by the District, District Data shall be Securely Destroyed when it is no longer needed for the designated purpose for which such data was disclosed to the Vendor. The Vendor agrees to provide documentation of data destruction to the District upon the District's reasonable request.

9. Change in Circumstances; Assignment

- a. Vendor will promptly notify the District in writing of any change in Vendor's or its employees', subcontractors', or agents' business or other circumstances that Vendor reasonably anticipates may affect District Data, including, but not limited to, any impending transfer or cessation of business or unlawful conduct. Vendor will reasonably cooperate with the District to minimize the effect of any such change in circumstances on the District, which may include, but is not limited to: (1) providing a full inventory of all District Data in the Vendor's, employee's, subcontractor's, or agent's actual or constructive possession, custody, or control and the location of same; (2) providing the District access to any Vendor facility, or reasonably assisting the District in obtaining access to other facilities and systems, as necessary to remove and Securely Destroy District Data or otherwise enforce the District's rights in and to District Data; and (3) upon the District's request, promptly transferring or Securely Destroying District Data, in whole or in part, as directed by the District.
- b. No assignment of this DPA or of any duty or obligation or performance hereunder, shall be made in whole or in part by either Party without the prior written consent of the other Party. In the event that a change in the Vendor's business circumstances, including, but not limited to, a merger, sale of company assets or shares, reorganization, financing, change of control, bankruptcy, or other corporate event, requires the assignment or other transfer of Vendor's rights, obligations, and/or liabilities with respect to District Data to a successor or other third party, prior to any such assignment or other transfer, Vendor must provide the District with written notice and an opportunity to object to such assignment or other transfer. The Parties will reasonably, and in good faith, collaborate to resolve the District's objection(s), if any; provided that:

- i. If the Parties are unable to resolve such objection to the District's satisfaction, notwithstanding any contrary provision of the Agreement, the District may terminate the Agreement, including this DPA, without penalty, liability, or further obligation to Vendor, and Vendor shall take commercially reasonable action to ensure a smooth transition of Services and transfer of District Data to the District or a third party designated by the District; and
- ii. If the District consents to such assignment or other transfer, any permitted successor or assign of the Vendor shall agree in writing to assume all of the Vendor's rights, interests, duties, obligations, and liabilities under this DPA prior to receiving access to District Data, and Vendor shall take all necessary actions to ensure a smooth transition of Services and/or transfer of District Data to such successor or assign.

10. Audits

- a. The District reserves the right, in its sole discretion, to perform audits of Vendor, at the District's expense, to ensure compliance with the terms of this DPA. The Vendor shall reasonably cooperate, and shall ensure that any Vendor employees, subcontractors, and agents reasonably cooperate, in the performance of such audits. Such audits shall only occur upon reasonable prior written notice to Vendor and in such a manner as to not unreasonably interfere with Vendor's operations.
- b. Vendor, or the data center(s) where Vendor maintains its systems and/or District Data, will, at Vendor's or such data center's expense, conduct or have conducted at least annually, a/an:
 - i. American Institute of CPAs Service Organization Controls (SOC) 2 Type II audit, or other commercially reasonable security audit, which attests the Vendor's or data center's security policies, procedures, and controls;
 - ii. Commercially reasonable vulnerability scan of the Vendor's or data center's electronic systems and facilities that are used in any way to provide Services or process or maintain District Data in connection with the Agreement; and
 - iii. Commercially reasonable formal penetration test of the Vendor's or data center's electronic systems and facilities that are used in any way to provide Services or process or maintain District Data in connection with the Agreement.
- b. Additionally, the Vendor shall provide the District, upon request, commercially reasonable summary results of the above audits and promptly modify its security measures as reasonably necessary based on those results in order to meet its obligations under the Agreement, this DPA, and applicable law.

11. Compliance

- a. Vendor warrants that the Vendor, its employees, and the Services shall be fully compliant, and will not adversely affect the District's compliance, with the relevant requirements of all state and federal laws, regulations, and guidance governing access to and use, maintenance, and disclosure of District Data. Vendor will use commercially reasonable efforts to ensure that Vendor's subcontractors and agents are fully compliant, and will not adversely affect the District's compliance, with the relevant requirements of all state and federal laws, regulations, and guidance governing access to and use, maintenance, and disclosure of District Data.
- b. Vendor warrants that any employees, subcontractors, and agents (including Contracted Third Parties) used by Vendor to provide the Services or otherwise fulfill Vendor's obligations under the Agreement will be subject to and will comply with the Agreement, this DPA, and applicable law in the same manner that Vendor itself is subject to the terms of the Agreement, this DPA, and applicable law.
- c. Except where a more stringent requirement is specified in the Agreement or this DPA, Vendor agrees to use commercially reasonable efforts to assist the District as necessary to maintain the security and confidentiality of District Data in accordance with the Agreement, this DPA, and applicable law.
- d. Upon the effective date of any amendment or issuance of laws, regulations, and guidance governing access to and use, maintenance, and disclosure of District Data, this DPA shall automatically be amended to conform with such requirements. Any ambiguity in this DPA shall be resolved in favor of a meaning that permits the District and Vendor, its employees, subcontractors, and agents to comply with any such laws, regulations, and guidance.

12. Term and Termination

- a. This DPA will become effective upon the Effective Date. Notwithstanding the termination of the Agreement, this DPA will continue in full force and effect until all District Data in the Vendor's, its employees', subcontractors', and agents' actual or constructive possession, custody, or control has been returned to the District or Securely Destroyed in accordance with Section 8.
- b. Notwithstanding any contrary provision of the Agreement, the District may immediately terminate the Agreement, including this DPA, for cause, without penalty, liability, or further obligation to Vendor, if the Vendor, its employee, subcontractor, or agent has breached a material term of this DPA and fails to cure such breach within ten (10) days after Vendor's receipt of written notice of such breach from the District; provided that, in the event that the breach is incapable of cure, the Agreement and/or this DPA shall terminate on the date specified in the District's notice.

13. Marketing/Advertisement

Vendor shall not use District Data for advertising or marketing purposes or to engage in any activity prohibited under Chapter 32, Texas Education Code, such as: (1) Targeted Advertising if the target of the advertising is based on any information acquired by Vendor for a School Purpose in connection with the Agreement, (2) marketing educational products directly to a student's parent if the marketing is the result of the use of information obtained by Vendor for a School Purpose in connection with the Agreement, (3) using information created or gathered by Vendor in connection with the Agreement to create a profile about a student for a purpose other than a School Purpose, or 4) selling or renting District Data. Any other use of District Data for advertising or marketing purposes shall be strictly prohibited unless Vendor has obtained the District's prior written consent.

14. Remedies

The Parties agree that, in addition to any legal or equitable rights and remedies of the District under the Agreement, this DPA, or applicable law, Vendor's, its employee's, subcontractor's, or agent's access to, or use, maintenance, or disclosure of (or threat to access, use, maintain, or disclose) any District Data in violation of the Agreement, this DPA, or applicable law shall be deemed to cause irreparable harm, for which monetary damages would not provide adequate compensation, that justifies injunctive relief against such breach or threatened breach without proving actual damage or posting a bond or other security. The Vendor further agrees to forfeit any fee(s) or other compensation payable by the District under the Agreement in the event the District terminates the Agreement for the Vendor's, its employee's, subcontractor's, or agent's material breach of any term of this DPA.

15. Amendment

The Parties may not alter or amend this DPA, except by written agreement properly executed by both Parties.

16. Entire Agreement

This DPA and the provisions of the Agreement, if any, directly concerning the security and confidentiality of District Data provided or otherwise made available to or gathered by the Vendor in connection with the Agreement constitute the entire agreement between the Parties regarding such subject matter and supersede any and all prior and contemporaneous representations, discussions, negotiations, and agreements—oral or written—by and between the Parties. The District expressly rejects any other agreements, terms, conditions, or policies, including, any terms of use, licensing agreements, privacy policies, or other agreements or understandings, that may be pre-published on any Vendor order acknowledgments, invoices, or forms, or otherwise proffered by Vendor or any third party in connection with the Agreement, whether electronic, click-through, verbal, or in writing, regardless of any agreement thereto by District employees or agents, and any such agreements shall be null, void, and without effect unless properly executed by the District and incorporated into this DPA in a valid amendment hereto.

17. Severability

If any provision of this DPA is determined to be illegal or unenforceable, then that provision shall be modified to the minimum extent necessary to render such provision legal and enforceable, and all remaining provisions shall remain in full force and effect.

18. Choice of Law/Venue

This DPA is made and is performable in Texas and shall be construed and enforced in accordance with, and shall be governed by, the laws of the State of Texas, without regard to choice of law principles. Any dispute arising from, related to, or in connection with this DPA shall be brought in a court of competent jurisdiction in Travis County, Texas, and the Parties hereby submit to and consent to the exclusive jurisdiction of said courts.

19. Headings

The headings in this DPA are for reference only and shall not affect the interpretation of this DPA.

20. Immunities

Nothing in this DPA shall be construed to create a claim or cause of action against the District for which it is not otherwise liable, nor to waive any immunity or defense to which the District, its trustees, officers, or employees may be entitled, nor to create an impermissible deficiency debt of the District.

21. Health Insurance Portability and Accountability Act

If the District determines that the Vendor, its employees, subcontractors, or agents will access, maintain, use, or disclose "protected health information" subject to the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub.L. 111-5) ("HITECH"), and/or the Texas Medical Records Privacy Act, Tex. Health & Safety Code Ann. § 181.001 *et seq.* ("TMRPA"), in addition to and as part of the terms and conditions of the Agreement and this DPA, the Parties agree to enter into a Business Associate Agreement, in form and substance reasonably agreeable to both Parties, providing for the privacy and security of such protected health information as required by HIPAA, HITECH, and the TMRPA, as such laws may be amended from time to time by the authorities having jurisdiction thereof.

IN WITNESS WHEREOF, the Parties have executed this DPA as of the Effective Date of the Agreement.

VENDOR: _____

By:

Printed Name: _____
Title: _____
Date: _____

EANES INDEPENDENT SCHOOL DISTRICT

By:

Printed Name: _____
Title: _____
Date: _____

EXHIBIT A to DATA PROTECTION ADDENDUM

Other types or categories of District Data:

[INSERT LIST, DATA FIELD, ETC. OR “None”]