TECHNOLOGY AND INFORMATION SERVICES

Proposed

Annual Technology Plan

Alhambra Unified School District

School Year: 2025-2026

Adopted:	*7/25/26*
Last Revised:	*6/22/26*
Next Review:	*26/27*

Table of Contents

Section 1: Vision and Governance
- 1.1 Purpose
- 1.2 Alignment with District Goals
- 1.3 Guiding Principles

Section 2: Resources and Access
- 2.1 Technology Resources
- 2.2 Equitable Access

Section 3: Teaching, Learning, and Safety
- 3.1 Improving Educational Services
- 3.2 Professional Development
- 3.3 Artificial Intelligence Use
- 3.4 Digital Citizenship, AI Literacy, and Misinformation
- 3.5 Cybersecurity and Privacy
  - Description:
  - Technical Safeguards:
  - Incident Response:
  - Phase
  - Actions
  - Primary Contact for Reporting Incidents:
  - Contact
  - Information

Section 4: Implementation
- 4.1 Priorities
  - Year
  - Priority
  - Status
- 4.2 Budget Summary
  - Category
  - Annual Allocation
  - Funding Source
- 4.3 Key Metrics
- 4.4 Review Schedule

Appendix A: BP 0440 Compliance Crosswalk

Related Documents

Section 1: Vision and Governance

1.1 Purpose

This Annual Technology Plan establishes how Alhambra Unified School District leverages technology to support its vision of creating safe, supportive, and reliable learning environments where all students can develop socially, emotionally, and academically. Developed in accordance with Board Policy 0440 (District Technology Plan), this document provides a comprehensive framework for the equitable deployment, responsible use, and continuous improvement of technology resources across all district operations—instructional, administrative, and infrastructure.

The plan guides district decision-making by defining the technology resources available to students and staff, ensuring equitable access across all school sites, aligning technology integration with research-based instructional strategies, and establishing expectations for cybersecurity, privacy, and responsible use. Updated annually by October, this plan serves as a living document that evolves with district priorities and emerging technologies while maintaining alignment with LCAP goals, board policy, state and federal requirements.

1.2 Alignment with District Goals

This technology plan directly supports the district's LCAP vision to create safe, supportive campuses where all students can develop socially, emotionally, and academically.

Technology investments and initiatives align with the four LCAP priority goals:

- **Attendance and Engagement:** The Student Information System(SIS) enables attendance monitoring for parents and staff, while CALPADS data systems identify chronic absenteeism patterns and trigger early intervention. Multilingual digital communications keep families connected to their child's school experience and support engagement across our diverse community.
- **Academic Achievement:** The district's 1:1 device program ensures every K-12 student has equitable access to digital learning tools. The Technology Continuum maps progressive skill development across grade levels, building digital research, data analysis, and multimedia creation competencies. Annual professional development equips educators to integrate technology effectively into instruction.
- **Social-Emotional Well-Being:** Digital citizenship instruction addresses internet safety, cyberbullying prevention, and digital wellness. Students learn to maintain a healthy screen-time balance and practice self-awareness when using digital tools, supporting overall well-being in an increasingly connected world.
- **Career and College Readiness:** Technology integration in CTE programs, combined with progressive digital literacy instruction, prepares students with the skills employers and post-secondary institutions expect. Students develop proficiency in ethical information use, collaboration tools, and emerging technologies, including artificial intelligence.
- **School Belonging and Safety:** Robust cybersecurity measures, content filtering, security camera systems, and modern public address (PA) systems support safe digital and physical environments across the district. The iSafe curriculum reinforces responsible online behavior, while clear acceptable use policies establish consistent expectations across all sites.

1.3 Guiding Principles

- Equity and access for all students and staff
- Student safety and privacy protection
- Responsible and ethical use of technology
- Research-based integration strategies
- Student-centered approach to technology adoption

Reference: AUSD 25-26 LCAP

Section 2: Resources and Access

2.1 Technology Resources

Category	Resources
Student Devices	Chromebooks (1:1 in grades 2-12; 2:1 in TK-1); HP Windows Laptops (CTE programs); Hotspots for qualified students with no internet access at home.
Staff Devices	HP Windows Laptops (certificated staff); HP Windows Desktops (support staff, administration); Document cameras; LCD projectors; ViewSonic interactive boards
Core Software	Google Classroom (LMS); Google Apps for Education, Microsoft Office Suite, Canva (productivity); Student Information System(SIS); iReady, Reading/Math Inventory, PowerTeacher Pro, Newsela, BrainPop, SeeSaw (assessment); Remind, Blackboard, Email, Smore Newsletters, Websites (communication)
AI Tools	AI platforms: ChatGPT, Microsoft Copilot, Gemini, MagicSchool.ai, NotebookLM.
Infrastructure	District-wide Wi-Fi 6E wireless network providing high-speed connectivity across all classrooms and common areas; fiber optic backbone connecting all 16 school sites; next-generation firewalls with advanced threat protection and content filtering; enterprise-grade storage and server virtualization supporting district applications; cloud-integrated backup system with disaster recovery capabilities; InformaCast emergency mass notification system for campus safety alerts and lockdown communication

2.2 Equitable Access

All 16 school sites maintain consistent technology access with 1:1 Chromebook deployment in grades 2-12 and 2:1 device ratios in TK-1 classrooms. District-wide Wi-Fi 6E connectivity ensures reliable network access across all instructional and common areas.

To address home connectivity gaps, the district provides mobile hotspots to qualified students who lack internet access at home, ensuring continuity of learning beyond the school day. For students with special needs, iPads and other assistive technology are deployed as specified in IEPs or 504 plans to support individualized learning needs.

The district monitors device access and connectivity through annual LCAP surveys and internal audits, adjusting resources as needed to maintain equitable access for all students, including foster youth, English learners, and low-income families.

Section 3: Teaching, Learning, and Safety

3.1 Improving Educational Services

Technology serves as a support tool for instruction, not the driver of instruction. The district prioritizes creating equitable, supportive learning environments through MTSS, strong relationships, responsive teaching, and data informed decision making with technology playing an important but complementary role in achieving these goals.

Digital tools enable progress monitoring, personalized learning pathways, and timely family communication. The district's Technology Continuum ensures students progressively develop digital literacy skills across grade levels, building research, analysis, and multimedia competencies aligned with college and career expectations. All technology initiatives are grounded in research based strategies and evaluated for effectiveness through multiple data systems including CALPADS, Student Information System(SIS), and the California Dashboard.

Goal	Technology Strategy	Measure
English Learner Program	Technology enables progress monitoring, data-driven instruction, family communication in home languages, and teacher collaboration to support language acquisition and academic achievement	ELPI reclassification rates; ELPAC proficiency levels; Smarter Balanced ELA performance gaps; A-G course enrollment for ELs
Educational Technology Training and Innovation	Technology integration through teacher professional development, boot camps, coaching, and pilot testing of emerging tools to enhance instructional effectiveness	PD completion rates; boot camp attendance; pilot testing outcomes; classroom integration observations; teacher self reported proficiency
Career Technical Education	Technology is embedded in industry-aligned pathways where students develop technical and digital skills for college and career readiness	CTE pathway completion rates; industry certifications earned; College/Career Indicator performance; dual enrollment and work-based learning participation

3.2 Professional Development

Alhambra Unified School District provides ongoing professional development to ensure all staff can effectively and responsibly integrate technology into instruction and operations. The district conducts an annual needs assessment survey to identify skill gaps and inform PD priorities. Training is delivered through multiple formats, including targeted workshops, collaborative site-based sessions, technology boot camps, and hands-on pilot testing of emerging tools. The Technology Committee, composed of teacher representatives from all sites, serves as a bridge between district goals and classroom practice, with members supporting peer mentorship and training across the district.

Audience	Focus Area	Delivery	Frequency
All Staff	Technology fundamentals, responsible use, data privacy, digital citizenship	Online modules, workshops, boot camps	Ongoing throughout the year
Teachers	Technology integration, curriculum-aligned digital tools, emerging platforms, (iSafe)	Workshops, boot camps, coaching, pilot testing	Ongoing throughout the year
New Hires	District systems orientation (Student Information System(SIS), Google Workspace, communication platforms)	Online modules	Upon hire
Technology Committee	Advanced technology training, planning, feedback, and technology evaluation	Collaborative sessions, vendor training	Ongoing throughout the year
Technology & Information Services Team	Technical skills, cybersecurity, infrastructure management, and emerging technologies	Vendor certifications, conferences, and hands-on training	Ongoing throughout the year

Reference: PD catalog and training calendar available through TIS; Contact training@ausd.us for scheduling

3.3 Artificial Intelligence Use

The use of artificial intelligence in Alhambra Unified School District is governed by Board Policy 0441(pending), which establishes nine guiding principles: student centered learning, staff support rather than replacement, ethical use and transparency, accountability and responsibility, equity and access, security and privacy, ongoing professional development, community engagement, and continuous improvement. These principles ensure AI enhances instruction while maintaining human judgment at the center of teaching and learning.

AI use also aligns with BP 4040 (Employee Use of Technology), BP 5131.9 (Academic Honesty), and BP 6163.4 (Student Use of Technology).

Who	Permitted Uses	Prohibited Uses	Disclosure
Students 9-12	Learning support and research; improving understanding of topics and concepts; brainstorming and idea generation; writing feedback and revision support; study aids and test preparation; coding assistance; language translation support; creativity aid; practicing digital literacy skills	Submitting AI-generated work as own; using AI during assessments unless permitted by teacher; entering personal information into AI tools; completing assignments with AI without teacher approval; bypassing content filters to access unauthorized AI tools; generating harmful, inappropriate, or misleading content	Cite AI tool used; describe how AI was used; follow teacher-specific citation guidelines
Students K-8	Teacher-directed activities only	Direct access to generative AI tools without teacher supervision; creating accounts on AI platforms; entering any personal information into AI tools	Verbally acknowledge AI was used; simple statement on assignment (e.g., "I used AI to help with this")
Staff	Lesson planning and differentiation; creating instructional materials and resources; generating assessment questions; administrative tasks (communications, reports, scheduling); professional learning and research; workflow efficiency	Entering student names, grades, or PII into public AI tools; using AI to make final decisions on grades, discipline, or placements without human review; using non-district-approved AI tools for student-facing activities; relying on AI output without verification for accuracy and bias; using AI-generated content without review and editing	Note AI assistance in professional documents when applicable; follow department or site guidelines

3.4 Digital Citizenship, AI Literacy, and Misinformation

Alhambra Unified School District integrates digital citizenship and online safety instruction across all grade levels through the iSafe curriculum, taught by staff to students in all classrooms. The iSafe program is a comprehensive school climate and student safety curriculum aligned to research from the American Institutes for Research and the National Center on Safe Supportive Learning Environments. Students learn to navigate the digital world safely, responsibly, and ethically—with instruction progressing from foundational online safety skills in early grades to advanced AI literacy and media analysis in high school.

The curriculum addresses three core areas: student engagement (identity, relationships, empowerment), student safety (emotional safety, physical safety, online safety, bullying and cyberbullying prevention, substance abuse awareness, risk prevention), and environment (school and classroom climate, online learning and social environments, health and well-being, guidance and discipline).

Grade Band	Focus Areas	Integrated In
K-2	Online safety, device care	All classrooms
3-5	Digital footprint, passwords, and reliable sources	All classrooms
6-8	Social media literacy, AI basics, misinformation	All classrooms
9-12	AI literacy, deepfakes, media analysis, and ethical use	All classrooms

Reference: iSafe and TIS Digital Citizenship Curriculum

3.5 Cybersecurity and Privacy

Description:

Alhambra Unified School District prioritizes the security and privacy of student and staff data across all digital systems. The district employs a multi-layered cybersecurity strategy that combines enterprise-grade infrastructure protections with ongoing user education and clear protocols for incident response.

Technical Safeguards:

Measure	Description
Next-Generation Firewalls	Redundant firewalls provide advanced threat protection.
Endpoint Detection and Response	SentinelOne provides managed EDR with real-time threat detection, automated response, and endpoint protection across district devices
Identity Management	Okta serves as the district's identity provider, enabling centralized authentication and multi-factor authentication (MFA) for staff
Phishing Awareness Training	Red Herring delivers phishing simulations to staff, building recognition skills and reinforcing security awareness
Backup and Disaster Recovery	Veeam Backup & Replication with dual on-premises and Azure cloud storage ensures rapid recovery capabilities
Content Filtering	Lightspeed Systems provides CIPA-compliant filtering and student activity monitoring
Network Monitoring	Real-time monitoring and automated alerting detect and respond to security incidents

Zero-Trust Roadmap	Zero-Trust Network Access (ZTNA) proof-of-concept planned for 2026-28 with phased implementation

Staff Training:

All staff complete mandatory cybersecurity awareness training at the beginning of each school year. This training covers password security, phishing recognition, data privacy responsibilities, and incident reporting procedures. Ongoing phishing simulations through Red Herring reinforce awareness throughout the year.

User Responsibilities:

Audience	Security Expectations
Students	Use strong, unique passwords; never share login credentials; recognize and report phishing attempts; report suspicious activity to a teacher or administrator; keep devices updated; do not install unauthorized software
Staff	Use strong, unique passwords; complete multi-factor authentication (MFA) via Okta; recognize and report phishing attempts; report security incidents to Technology and Information Services; keep devices updated; do not install unauthorized software or access district systems on unapproved devices

Incident Response:

The district maintains a Cybersecurity Incident Response Plan to ensure a rapid, coordinated response to security events. The plan covers phishing and social engineering attempts, malware and ransomware, unauthorized access to systems or data, data breaches involving student or staff personally identifiable information, lost or stolen devices, and denial-of-service attacks.

Phase	Actions
1. Reporting	Staff report suspected incidents immediately by notifying their supervisor, submitting a help desk ticket, or contacting the Director of Technology directly
2. Assessment	The Director of Technology assesses the incident and classifies its severity (Low, Medium, High, or Critical). The Superintendent and district legal counsel are notified immediately for High or Critical incidents. For significant incidents, the district contacts its cyber insurance provider within 24 hours and engages an external Incident Response Team. Additional resources are coordinated as needed with the Los Angeles County Office of Education (LACOE), Cybersecurity and Infrastructure Security Agency (CISA), and the California Governor's Office of Emergency Services (CalOES) Cybersecurity Division. The FBI is notified for incidents involving criminal activity or critical infrastructure. All incidents are documented and reviewed to improve future response

3. Containment & Notification	The Technology Department coordinates with the district's Public Information Officer to develop communications throughout the incident response process. Once the incident is contained, notifications are issued to affected parties via email, website posting, and direct mail as appropriate. All communications are reviewed by the Incident Response Team, legal counsel, senior AUSD leadership, and the cyber insurance provider to ensure compliance with FERPA and California Civil Code 1798.82.
4. Recovery & Review	Systems are verified clean and restored from backup, with critical services prioritized. All affected credentials are reset. The district conducts a formal after action review to document lessons learned, evaluate response effectiveness, and identify improvements. Policies and procedures are updated as needed, and findings are reported to the Board. Evidence is preserved for potential legal or law enforcement purposes.

Contact	Information
Ashton Potter, Director of Technology	potter_ashton@ausd.us

Privacy Protections:

All technology use complies with Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy Protection Act (COPPA), and Student Online Personal Information Protection Act (SOPIPA). The district reviews vendor agreements to ensure student data is protected and used only for authorized educational purposes. Data collection is limited to what is necessary for educational and operational needs. Access to student and staff data is restricted based on role and job function. Sensitive data is encrypted in transit and at rest. Parents are informed of their rights regarding student records and may request access to or corrections of student records in accordance with Board Policy 5125.

Section 4: Implementation

This section outlines how the district will execute the technology plan. Annual priorities are tracked for progress, and budget allocations are aligned with the district's Local Control and Accountability Plan (LCAP). The LCAP serves as the primary planning and budgeting framework, ensuring technology investments support district goals for student achievement, equity, and engagement.

4.1 Priorities

Year	Priority	Status
2025-26	AI Board Policy Adoption (0441)	In Progress
2025-26	Device Refresh	On Track
2025-26	Infrastructure Upgrades	On Track
2025-26	IT Support Services	In Progress

4.2 Budget Summary

Category	Annual Allocation	Funding Source
Technology Staff	$1,744,965.00	*General Funds*
Technology Support of Unduplicated Pupils	$2,916,878.00	*General Funds*
Technology Operations	$182,001.00	*General Funds*
Technology Infrastructure	$626,864.00	*General Funds*
Cybersecurity	*$377,730.00*	*General Funds*
Staff & Student Technology Systems	*$2,180,156.00*	*General / Bond Funds*

Reference: AUSD 25-26 LCAP

4.3 Key Metrics

Metric	Description
Device access ratio by site	1:1 student-to-device ratio for grades 2-12; 2:1 for TK-1
Cybersecurity incident count	Number of security incidents reported annually
Network uptime percentage	Target ≥99.9% availability
Help desk ticket resolution time	Average time to resolve Tier 1 tickets
E-Rate funding secured	Annual E-Rate reimbursements received
Technology training engagement	Number of sessions offered and total staff participation in district technology training
iSafe module completion	Completion of iSafe modules downloads by school sites

4.4 Review Schedule

Description:

The District Technology Plan is a living document reviewed annually to ensure continued relevance and effectiveness. Community feedback is collected during the annual LCAP review and update meeting. Staff and student input is gathered throughout the year. This feedback drives each revision, ensuring the plan remains responsive to district needs and priorities. The review cycle begins at the end of each school year with data collection, continues with drafting over the summer, and concludes in September with leadership approval. The revised plan is published by CBEDS Information Day each October.

Review Activity	Frequency	Responsible Party
Community feedback collection (LCAP), Community surveys	Annual	Director of TIS, Tech Trainers
Metrics review	Annual	Director of TIS, Tech Trainers, TIS
Plan review and update	Annual	Technology Committee, TIS
Management team feedback	Annual	Director of Technology
Board update	Annual	Director of Technology

AI Acknowledgment

AI tools were used to support the development of this plan. All content has been reviewed and approved by AUSD staff.

Appendix A: BP 0440 Compliance Crosswalk

BP 0440 Requirement	Plan Section
Technological resources utilized	2.1
Equitable accessibility	2.2
Improve educational services	3.1
Professional development	3.2
AI use aligned with BP 0441, 4040, 5131.9, 6163.4	3.3
Digital citizenship, social media, AI literacy, misinformation	3.4
Cybersecurity prevention and response	3.5
Privacy and confidentiality	3.5
Integration with district vision and goals	1.2
Research-based strategies	3.1

Related Documents

This plan references and should be used in conjunction with:

- BP 0440 - District Technology Plan
- BP 0441 - Artificial Intelligence
- BP 4040 - Employee Use of Technology
- BP 5131.9 - Academic Honesty
- BP 6163.4 - Student Use of Technology
- Parent / Student Handbook
- Cybersecurity Incident Response Plan
- *[Data Governance Handbook] (coming soon)*