HAMILTON UNIFIED SCHOOL DISTRICT

Department of Technology | Technology Acceptable Use Agreement & Device Policy (SY 2026–2027) — Page 1

Note: Operational configurations, approved applications, and security settings may change during the school year in response to operational, educational, legal, or cybersecurity requirements.

1. AUTHORIZATION, PURPOSE & DISTRICT OWNERSHIP

Hamilton Unified School District (HUSD) authorizes students and staff ("users") to access district technology resources—including network infrastructure, Chromebooks, Google Workspace accounts, internet access, and educational software—solely for legitimate instructional and administrative purposes. Technology access is a privilege permitted at the District's discretion, subject to Board Policy BP 4040, Administrative Regulations, and this Acceptable Use Policy (AUP).

District Ownership: All computers, network infrastructure, mobile devices, electronic user accounts (`@husdschools.org`), and created/stored files remain the exclusive property of Hamilton Unified School District. The District reserves the right to collect, inspect, alter, or revoke access to any district technology at any time without prior notice.

2. MANAGED SECURITY CONTROLS, ACCOUNT CONFIDENTIALITY & APP CONTROLS

To support student privacy and safeguard district networks against cyber threats, HUSD enforces a managed security control model (Zero Trust framework):

- **Account Confidentiality:** Users are solely responsible for their assigned accounts. Passwords must remain strictly confidential. Account sharing or accessing another individual's account is strictly prohibited.
- **Managed Application Controls:** Student accounts are restricted from authenticating external third-party applications via Google Sign-In or OAuth without prior IT approval. External instructional software must undergo IT privacy review and align with California Student Data Privacy Agreements (CA-NDPA).
- **Prohibited Automation Add-Ons:** Unapproved third-party email automation tools, mail merge add-ons, and unverified browser extensions are blocked domain-wide to reduce phishing and email spoofing risks.
- **Approved Registry:** The complete list of district-approved tools is maintained live at: **https://www.husdschools.org/departments/technology/approved-third-party-google-apps**

3. GENERATIVE ARTIFICIAL INTELLIGENCE (GENAI) GOVERNANCE

HUSD recognizes the educational value of Artificial Intelligence while maintaining rigorous privacy and instructional guardrails:

- **Official District Platform: Gemini in Google Workspace for Education** (managed under HUSD accounts) is the District's officially approved generative AI tool. Workspace data processed via Gemini is excluded from public AI model training.
- **Human-in-the-Loop Standard:** AI tools serve to augment, not replace, human critical thinking and educator judgment. All AI-generated outputs must be reviewed and verified for accuracy before use.
- **Strict Data Prohibitions:** Users are strictly forbidden from inputting student Personally Identifiable Information (PII) (e.g., student names, IDs, addresses, IEP data), confidential employee records, disciplinary records, medical information, legal documents, or attorney-client communications into any AI platform.
- **Prohibited Consumer AI:** Unvetted, consumer-grade AI tools (e.g., consumer ChatGPT, Claude, unapproved grading bots) are blocked for students and restricted for staff to prevent commercial data collection.

Note: Operational configurations, approved applications, and security settings may change during the school year in response to operational, educational, legal, or cybersecurity requirements.

4. EXTERNAL CONTENT & FILE IMPORT PROTOCOL ("FLATTENED COPY" WORKFLOW)

To mitigate active macro malware and unvetted background code execution from crowdsourced file repositories (e.g., Teachers Pay Teachers / TPT):

> **Sanitized File Import Requirement:** Staff purchasing or downloading third-party instructional materials on personal home devices must convert files into static, flattened copies (e.g., "Print to PDF" or "Save as Picture/JPEG") prior to transferring them to school computers. Direct Google Drive account linkage to external crowdsourced marketplaces is prohibited.

5. DIGITAL CITIZENSHIP, SAFETY & LEGAL COMPLIANCE

Users must adhere to high standards of digital citizenship. The following conducts are strictly prohibited and constitute policy violations:

- **Harmful & Obscene Material:** Accessing, creating, or disseminating material that is obscene, sexually explicit, discriminatory, or harmful to minors (Cal. Penal Code 313).
- **Cyberbullying & Harassment:** Threatening, intimidating, or harassing students, staff, or community members via email, shared Docs, chat, or online platforms.
- **Unauthorized System Access ("Hacking"):** Attempting to bypass web filters, alter system configurations, elevate privileges, run network exploits, or access confidential student record systems (Cal. Penal Code 502).
- **Commercial Use & Copyright:** Utilizing district networks for personal commercial gain, political lobbying, or unauthorized downloading of copyrighted media.

6. PRIVACY EXPECTATIONS & TECHNOLOGY MONITORING

Privacy Expectations: District-owned devices, accounts, and networks are subject to monitoring, inspection, and logging for legitimate educational, operational, and security purposes. Users should not expect personal privacy when using District technology resources. Monitoring tools include:

- **Palo Alto Next-Generation Firewall:** Network traffic inspection and web filtering.
- **GoGuardian Classroom & Safety Systems:** Real-time screen visibility, activity logging, and safety alerts.
- **Endpoint & API Security:** Endpoint threat protection and Google Admin administrative logs.

Note: Operational configurations, approved applications, and security settings may change during the school year in response to operational, educational, legal, or cybersecurity requirements.

7. CHROMEBOOK & DEVICE STANDARDS OF USE & DAMAGE FEE SCHEDULE

Students assigned a HUSD-owned Chromebook or device must adhere to care standards: bring the device fully charged daily in its protective case, do not leave devices unattended or place stickers/markings on hardware, and report loss or physical damage to the school office immediately.

HUSD Chromebook / Device Damage Fee Schedule (SY 2026–2027)

Incident / Offense Tier	District Coverage Share	Parent / User Fee Responsibilities
1st Offense (Accidental)	District covers 100% of repair / replacement cost.	**$0 Fee** (Full Device, Charger, Screen, Keyboard)
2nd Offense (Repeated)	District covers 50% of repair / replacement cost.	Full Device: **$200** | Screen: **$75** | Keyboard: **$50** | Charger: **$25**
3rd Offense & Intentional Abuse	User responsible for 100% of repair / replacement cost.	Full Device: **$400** | Screen: **$150** | Keyboard: **$100** | Charger: **$50**

Student & Parent/Guardian Agreement Signature Block

I have read, understand, and agree to abide by the terms of the HUSD Technology Acceptable Use Policy and Device Agreement for SY 2026–2027. I understand that violation of these rules may result in revocation of technology privileges, disciplinary action, or financial responsibility for damaged equipment.

Student Printed Name: _____ **Grade Level:** _____

Student Signature: _____ **Date:** _____

Parent/Guardian Printed Name: _____

Parent/Guardian Signature: _____ **Date:** _____