



479 TOWNSHIP ROAD 1902
JEROMESVILLE, OHIO
44840

www.hillsdale.k12.oh.us

HILLSDALE PK-6
419-368-4364

HILLSDALE 7-12
419-368-6841

CENTRAL OFFICE
419-368-8231

Hillsdale Local School District Staff Acceptable Use Policy (AUP) 2025-2026

Overview

The Hillsdale Local School District (HLSD) is committed to providing staff with the technology necessary for professional and instructional use while ensuring compliance with Ohio Senate Bill 29 (SB 29), Ohio House Bill 432 (HB 432), the Student Information Protection Act (SIPA), the Children's Internet Protection Act (CIPA), and Board policies. All HLSD staff members are expected to use district technology resources responsibly, ethically, and securely to support the district's educational mission. By using HLSD technology and network resources, staff agree to adhere to this Acceptable Use Policy (AUP) based on Board Policy EDE and acknowledge their role in maintaining a safe and secure digital environment.

Use of District Technology and Network Resources

HLSD provides district-owned computers, tablets, network access, software, cloud services, and other digital resources to facilitate teaching, administrative tasks, and communication. Staff use of district technology must:

- Support instruction, research, professional development, and administrative functions.
- Comply with Board Policy EDE: Computer/Online Services (Acceptable Use and Internet Safety).
- Adhere to state and federal laws governing data security, digital communication, and content access.

Prohibited Activities

Staff members may not use district technology for:

- Personal financial gain, commercial activity, or unauthorized fundraising.
- Accessing or distributing inappropriate, obscene, or offensive materials.
- Unauthorized access to or tampering with district systems, student/staff records, or confidential information.
- Cyberbullying, harassment, or any form of discriminatory behavior.

Monitoring & Security Measures

To ensure compliance and security, HLSD:

- Monitors staff internet activity and device usage through IBOSS and other cybersecurity tools.
- Prohibits personal devices from connecting to the district network to protect data integrity.
- Maintains content filtering and data encryption to prevent unauthorized access or exposure to harmful content.

- Conducts routine security audits and compliance checks to safeguard sensitive data and network infrastructure.

Staff must report security concerns, breaches, or suspicious activity immediately to the Technology Department or Administration.

Artificial Intelligence (AI) Use

HLSD acknowledges the growing role of Artificial Intelligence (AI) in education and requires that all AI use aligns with Board Policy EDEC on AI. Staff must:

- Use AI tools ethically and responsibly in instructional and administrative activities.
- Ensure AI-generated content is properly attributed and not misrepresented as original work.
- Avoid entering confidential student or staff information into AI systems.
- Guide students through the proper use of AI in the classroom.

Misuse of AI, including violations of academic integrity, security policies, or ethical guidelines, may result in disciplinary action.

Data Privacy & Compliance

HLSD staff must handle student and staff data in accordance with SIPA, CIPA, and FERPA to ensure privacy and security. Staff are required to:

- Follow data encryption and access control protocols when handling sensitive information.
- Use district-approved applications to store and share educational records.
- Report data breaches or unauthorized access immediately.
- Ensure compliance with third-party vendor agreements, which require providers to delete student data within 90 days after contract expiration.

Cybersecurity Responsibilities

Cybersecurity is a shared responsibility among all HLSD staff members. To minimize risk:

- Staff must use strong passwords and multi-factor authentication where applicable. All staff must have a minimum of 15 characters for a password.
- Unauthorized software installation on district devices is strictly prohibited.
- Staff must log out of devices when not in use and store them securely.
- Phishing emails, malware, and other cybersecurity threats must be reported immediately.

Violations & Consequences

Failure to comply with the HLSD Staff AUP may result in:

- Revocation of technology access or device privileges.
- Disciplinary action, including suspension or termination.
- Legal consequences if state or federal laws are violated.

By signing this policy, staff acknowledge their understanding of an agreement to abide by the HLSD Staff Acceptable Use Policy and all related Board policies.

Acknowledgment & Signature

I have read and understood the **Hillsdale Local School District Staff Acceptable Use Policy (AUP)** and agree to comply with all its requirements.

Name:

Position:

Signature:

Date: _____

For questions regarding this policy, contact the HLSD Technology Department.