LIBERTYVILLE
SCHOOL DISTRICT #70

1381 West Lake Street
Libertyville, IL 60048
Phone: (847) 362-9695
Fax: (847) 362-3003
d70schools.org

Staff Acceptable Use Procedures & Guidelines (AUPG)

Purpose & Scope

Libertyville School District 70 provides technology resources to support educational excellence, enhance operations, and facilitate professional communication. This Acceptable Use Policy & Guidelines (AUPG) outlines the standards of acceptable, ethical, and secure use of all district-owned technology, networks, and communication tools.
This policy applies to all full-time, part-time, temporary, and contracted staff members. Compliance with this policy aims to protect individual staff members from liability and safeguards the district's students, data, and infrastructure.

1. Student Data Privacy & Legal Compliance (FERPA, COPPA, & SOPPA)

As an Illinois school district, we are legally mandated to strictly protect student data privacy under federal and state laws, including the Family Educational Rights and Privacy Act (**FERPA**), the Children's Online Privacy Protection Act (**COPPA**), and the Illinois Student Online Personal Protection Act (**SOPPA**).

- **Unauthorized Platforms:** Staff are strictly prohibited from entering, uploading, or tracking student Personally Identifiable Information (PII), including names, grades, ID numbers, demographics, or academic records, into any website, software, application, or cloud service not explicitly approved and vetted by the District Technology Department.
- **SOPPA Compliance & Vendor Agreements:** Under SOPPA, the district must have a signed Data Privacy Agreement (DPA) in place with any operator before student PII can be utilized. Staff may only use digital tools listed on the district's approved SOPPA clearinghouse website. If a tool is not explicitly approved, do not create an account or input data.

2. Official Communication & Social Media Boundaries (Ref: Board Policy 5:125)

As employees of a public school district, staff members represent the district at all times. To protect both students and staff, strict boundaries must be maintained regarding digital engagement.

- **No Official Capacity on Personal Social Media:** Staff members shall not use personal social media accounts (e.g., Facebook, Instagram, X/Twitter, TikTok, etc.) in an official capacity as a representative of the district, school, or classroom.
- **Approved Engagement Channels:** In an effort to maximize student and staff safety,

ParentSquare, **RingCentral** and **District Google Email** are the only approved methods for communicating and engaging with families. Do not create separate social media groups, pages, or accounts for your classroom, club, or sports team.
- **District-Sanctioned Accounts:** The district and individual school buildings may continue to maintain official, centralized social media presences managed by authorized administrative personnel.

3. District Branding and Mascot Usage (Ref: Board Policy 5:125)

All external and digital communications serve as a reflection of the district's professional identity.
- **Branding Guidelines:** Any and all digital communications, including but not limited to ParentSquare broadcasts, district emails, digital newsletters, and official presentations, must strictly adhere to the **District Branding Guidelines**.
- **Mascot and Logo Usage:** Staff must only use approved, high-resolution versions of the district/school mascot and logos as outlined in the branding guide. Altering, stretching, or using unauthorized, modified versions of the mascot or logos is prohibited.

4. Artificial Intelligence (AI) Usage

The district recognizes the emerging role of artificial intelligence in education.
- **Separate Guidance:** This AUPG acknowledges that the district maintains a **separate, supplemental guidance document regarding AI usage** for staff.
- **Data Security:** Under no circumstances should student PII, student photos, confidential district data, or proprietary curriculum materials be entered into public AI models (e.g., open-source chatbots, image generators)

5. Data Security

- Staff members are required to utilize Multi-Factor Authentication (MFA) for all District systems where it is made available, including but not limited to email, network access, and student information systems. Staff members shall not attempt to bypass or disable MFA protections. Repeated or suspicious authentication requests must be reported immediately to the Technology Department.
- Staff members shall not install, access, or utilize third-party applications, software, browser extensions, or Software-as-a-Service (SaaS) platforms that interact with District data or systems without prior approval from the Technology Department.
- Staff members shall be responsible for reporting suspected or actual breaches of data security. Such incidents include, but are not limited to phishing attempts, unauthorized access, accidental disclosure of sensitive information (including student record information), lost or stolen devices, or suspicious system activity. All incidents must be reported immediately to the Technology Department, and staff members shall not attempt to independently remediate or conceal such incidents.
- Staff members are prohibited from entering, uploading, transmitting, or otherwise disclosing personally identifiable information (PII), including student record information, and other sensitive information related to students or staff into any AI or other system that is not expressly approved by the District.

6. Student Photography and Media (Ref: Board Policy 5:125)

To protect student privacy and mitigate digital safety risks, strict boundaries are enforced regarding media capture.

- **Personal Devices:** Staff members are **not permitted** to take photographs, record videos, or capture audio of students on personal devices (e.g., personal smartphones, tablets, smartglasses, or cameras).
- **Approved Capture:** Any digital media of students for school, classroom, or district purposes must be captured using **district-owned devices**.
- **Media Release:** Prior to publishing any student media on approved district channels, staff must verify that the student has a valid media release on file.

7. Approved Communication Channels (Ref: Board Policy 5:125)

To maintain professional boundaries, transparency, and reliable archiving, all work-, school-, or district-related communications with colleagues, families, and students must flow exclusively through the following approved platforms:

Approved Platform	Authorized Use Case
District Google Workspace Accounts	Official email (@d70schools.org), internal collaboration, lesson planning, and direct professional peer-to-peer communication.
ParentSquare	All mass broadcasts, classroom updates, direct messaging to families/parents, and official school-to-home outreach.

- **Prohibited Communication:** The use of personal email accounts, personal phone numbers (texting/calling), unapproved messaging apps, or personal social media accounts to conduct district business or communicate with students/families is strictly prohibited.

8. Personal Technology Usage (Ref: Board Policy 5:125)

Staff members are expected to focus on professional duties during work hours. The use of personal technology (e.g., smartphones, tablets, smartwatches) for personal purposes is permitted only during non-work, duty-free times. Usage must not interfere with job responsibilities or disrupt the school environment.

9. Accountability and Disciplinary Action (Ref: Board Policies 5:120, 5:125)

The use of district technology resources is a privilege, not a right. The district reserves the right to monitor, log, and access all data on district-owned networks and devices to ensure safety and compliance.

- **Non-Compliance:** Failure to adhere to the guidelines outlined in this AUPG may result in the limitation or revocation of technology privileges.
- **Disciplinary Procedures:** Violations of this policy will be investigated and may result in **disciplinary action, up to and including termination of employment**, as well as potential legal or civil liability depending on the severity of the infraction.

Staff Acknowledgment & Sign-Off

I acknowledge that I have received, read, and understand the Libertyville District 70 Staff Acceptable Use Policy & Guidelines (AUPG), including compliance mandates for FERPA, COPPA, and Illinois SOPPA. I agree to abide by these terms, including the restrictions on personal device student photography, social media usage, branding guidelines, and approved communication channels, as a condition of my employment. I understand that a separate supplemental guidance document exists for AI usage and that I am responsible for adhering to those guidelines as well.

Staff Name (Printed): _____

Date: _____