



# LYNCHBURG CITY SCHOOLS TECHNOLOGY USE GUIDELINES

**Board Policy Reference:** Policy IIBEA/GAB (Acceptable Computer System Use)

**Department:** Department of Information Technology

## 1. Purpose

The Lynchburg City Schools (LCS) Board provides students and staff access to a variety of technological resources to promote educational excellence. These resources provide opportunities to enhance learning, appeal to different learning styles, and improve communication within the school community and the larger global community.

Through the school system's technological resources, users can observe events as they occur around the world, interact with others on a variety of subjects, and acquire access to current and in-depth information. The use of these resources is a **privilege, not a right**.

## 2. Definition of Technological Resources

These guidelines apply to all technology provided by the district, as well as personal devices when used on school property or to access school resources.

**"Technological Resources" include, but are not limited to:**

- **Hardware:** Computers, tablets, laptops, servers, printers, projectors, and multimedia devices.
- **Networks:** Wired and wireless internet connections, internal networks, and cloud storage systems.
- **Communication Tools:** Email, learning management systems, and authorized social media platforms.

- **Wearables:** Smartwatches, smart eyeglasses (e.g., Ray-Ban Stories), fitness trackers, and VR headsets.
- **Personal Devices:** Smartphones and personal laptops when connected to the LCS network.

## 3. User Responsibilities & System Security

Users play a critical role in maintaining the security of the LCS network. You are responsible for your behavior and communications when using these resources.

### A. Account Security

- **Password Protection:** Users must not share their passwords or account credentials with anyone. You are responsible for all activity that occurs under your account.
- **Authorized Access:** Users are prohibited from using another individual's ID or password without express permission.
- **Reporting Vulnerabilities:** If a user identifies a security problem or vulnerability (e.g., a way to bypass a filter), they must **immediately** notify a teacher or administrator. Users **must not** demonstrate the problem to others.

### B. Data Stewardship

- **Backups:** LCS provides digital storage; however, no server is 100% reliable. It is the user's responsibility to back up important data and files.
- **Malicious Software:** Users may not knowingly or negligently transmit computer viruses, or create/introduce games or network communication programs without permission from the Technology Director.

## 4. Privacy and Monitoring

LCS balances the need for a safe environment with user access. However, users must understand the following regarding privacy:

- **No Expectation of Privacy:** Students and staff have **no expectation of privacy** in anything they create, store, send, or receive on the school system's network or devices. This applies even if the content is personal in nature.
- **Right to Monitor:** School officials may monitor, read, and archive email, files, browsing history, and system outputs at any time without prior notice to ensure system integrity and compliance with policy.
- **Public Records:** Electronic data stored on school computers may be considered public records and subject to disclosure under state law or legal proceedings.

## 5. Digital Citizenship & Prohibited Activities

Users are expected to abide by generally accepted rules of network etiquette and conduct.

### A. Prohibited Actions

- **Circumvention:** Using proxies, VPNs, or hotspots to bypass LCS content filters is strictly prohibited.
- **Unlawful Activities:** "Hacking" or attempting to gain unauthorized access to other computers or systems is forbidden.
- **Commercial Use:** Using school resources for commercial gain, profit, or political campaigning is prohibited.
- **Bullying & Harassment:** Users may not create or transmit material that is obscene, defamatory, profane, threatening, or considered harmful to minors.
- **Deep Fakes / Cloning / Mimicry:** Students shall refrain from using artificial intelligence to generate a likeness or similarity (visual or auditory) to any other person without first obtaining the person's consent as well as permission from their teacher.

### B. Wearables and Recording

- **Smart Eyeglasses:** To protect the privacy of others, smart glasses capable of recording video or audio are prohibited during assessments and in private areas (restrooms, locker rooms).
- **Recording Consent:** Students may not use technology to capture audio, video, or still pictures of others without their consent and the approval of a school administrator.

## 6. Generative AI

### A. General use

- **Prohibited:** Students may use only pre-approved generative AI tools in the use of their studies. Any other classroom use is strictly prohibited.
- **Allowed/Encouraged Use:** AI is allowed for high-quality instruction and learning standards and practices

### B. Classroom Guidance

- **Guardrails & Safety:** Students will always follow the direction of their teacher in their use of AI.

- **Traffic Light System:** Teachers will establish a traffic light system for lessons and curriculum activities in their classrooms.
  - Red = No use of AI
  - Yellow = Partial use of AI (as a thought partner or as directed by their teacher)
  - Green = Full use of AI, but the student is required to cite sources, prompts, and clearly explain how and why they used AI

## 7. Academic Integrity

Technology should foster authentic learning.

- **Plagiarism:** Plagiarism of internet resources will be treated in the same manner as traditional plagiarism found in the Code of Student Conduct.
- **Copyright:** Users must respect copyright laws. Unauthorized copying of software or media is prohibited.

## 8. Consequences of Misuse

Failure to adhere to these guidelines will result in disciplinary action. This may include the limitation or revocation of user privileges, suspension or expulsion for students, termination for employees, and referral to law enforcement for criminal prosecution where applicable.

---

**Footer** *LCS Technology Use Guidelines | Policy Code: IIBEA/GAB*

**Revision History**