

NORTH PROVIDENCE PUBLIC SCHOOLS STAFF COMPUTER & TECHNOLOGY RESOURCES AUTHORIZED USER POLICY	Approved: 5/27/2020 Updated: 8/26/2026

I. PURPOSE AND COMPLIANCE

The North Providence Public Schools recognizes that computers, electronic communications, network infrastructure, and Internet access systems are vital tools for assisting District employees and authorized users in providing public education and operational services.

The primary purpose of this policy is to balance the need for robust technology resources with the District's mandate to maintain professionalism, secure sensitive information, and ensure an ethical, legal environment.

All technology resources provided by the District are the exclusive property of North Providence Public Schools. Accordingly, all data and communications created, received, or stored on these systems are subject to monitoring, and users have **no expectation of privacy**.

This policy ensures District compliance with all applicable federal, state, and local mandates governing digital privacy, civil rights, and data security. Authorized use of District technology systems shall be aligned with, and restricted by, requirements including but not limited to:

- **Student Privacy & Education Rights:** The Family Educational Rights and Privacy Act (**FERPA**), the Children's Online Privacy Protection Act (**COPPA**), the Protection of Pupil Rights Amendment (**PPRA**), and the Individuals with Disabilities Education Act (**IDEA**).
- **Civil Rights & Equity:** **Title VI** of the Civil Rights Act of 1964 and **Title IX** of the Education Amendments of 1972.
- **Internet Safety & Data Security:** The Children's Internet Protection Act (**CIPA**), the Health Insurance Portability and Accountability Act (**HIPAA**), and the Rhode Island Identity Theft Protection Act (**R.I.G.L. § 11-49.3**).

II. SCOPE

This policy applies to all technology resources owned, leased, or sponsored by the District, including hardware, software, network infrastructure, wired and wireless connections, electronic mail, phone networks, and shared data spaces.

The scope extends to:

- All authorized users, including full-time, part-time, temporary, and contract employees, as well as consultants, volunteers, and external vendors.

- All District-owned devices used either on or off District premises, during or outside of normal working hours.
- Personal devices connecting to the District network under Bring Your Own Device (**BYOD**) provisions.

III. USER EXPECTATIONS & CORPORATE BUSINESS

All authorized users are expected to utilize District technology resources in an ethical, legal, and responsible manner to carry out legitimate school department business.

- **Official Communications:** All electronic correspondence concerning School Department business - including communication with students, parents/guardians, medical professionals, and public officials - must be executed exclusively through District-provided accounts. The use of personal email accounts or personal SMS/messaging applications for official business is strictly prohibited.
- **Data Protection & AI:** Users are explicitly prohibited from inputting student Personally Identifiable Information (PII), student images, confidential records, or medical information into unapproved third-party or personal Generative AI tools.
- **Copyright Compliance:** Users must respect intellectual property rights, copyright laws, and licensing agreements when accessing or distributing materials via the District network.

IV. ADMINISTRATIVE REGULATIONS & ENFORCEMENT

The Superintendent, or their designee, is authorized to establish detailed operational protocols, regulations, and user requirements to implement this policy.

- **System Monitoring:** The District reserves the right to manage, audit, and monitor its networks, electronic communication platforms, and device data to maintain system security and ensure compliance.
- **Violations:** Any violation of this policy or its associated protocol may result in the restriction or loss of technology privileges, progressive disciplinary action up to and including termination in accordance with collective bargaining agreements, or referral to law enforcement officials when federal or state laws are breached.

[Staff Computer/Technology Resources Authorized User Protocol](#)

Approved: 5/27/2020

Updated: 9/20/2024

Updated: 8/26/2026