

Use of Technology Resources in Instruction

The Bristol Warren Regional School District (“BWRSD” or “District”) provides technology resources to support teaching, learning, accessibility, communication, student services, and District operations. All users are expected to use these resources safely, securely, responsibly, and ethically.

Scope & Other Policies

- **Who it applies to:** Students, staff, volunteers, contractors, and guests using any District-owned or personal device connected to District networks, accounts, or data.
- **Related policies:** Works alongside policies for student equipment (**JFBC/JFBC-E**), information security (**EHAA**), and artificial intelligence (**IJNDB**), as well as handbooks, codes of conduct, union contracts, IEPs, and 504 plans.

1. Authorized & Responsible Use

District technology is meant for educational and operational purposes, including approved clubs, teams, and events. Staff may use technology for limited personal use if it does not interfere with work, incur costs, or pose security risks.

Users shall:

- Use only accounts, devices, systems, and applications they are authorized to access;
- Protect passwords, authentication methods, and other credentials;
- Use only District-approved tools and communication methods for protected or confidential information;
- Promptly report suspected phishing, malware, account compromise, data loss, or other cybersecurity incidents;
- Respect privacy, copyright, intellectual property, and academic integrity requirements;
- Preserve District records as required by law, policy, or administrative procedure; and
- Follow reasonable technology and security instructions issued by authorized District personnel.

2. Prohibited Uses

Unless explicitly authorized for official technical or security reasons, **users must not:**

- Engage in illegal acts, bullying, harassment, fraud, cheating, or plagiarism.
- Attempt unauthorized access to systems, files, or accounts, or impersonate others.
- Share, steal, or capture passwords, multi-factor authentication codes, or encryption keys.

- Test systems for vulnerabilities without tech approval, spread malware, or bypass security/monitoring settings.
- Use unauthorized VPNs, proxies, or alternate OS/developer modes to dodge filtering.
- Modify, delete, or share another person's or District data without permission.
- Use technology for commercial gain, private business, or cryptocurrency mining.

3. Privacy, Personal Devices, & Monitoring

- **Data protection:** Personal and protected data must only be used in approved apps. AI tools must comply with policy **IJNDB**.
- **Personal devices:** Subject to filtering and security rules when connected. Connecting a personal device does not give the District open access to personal content, but District accounts and network traffic are subject to logging and review.
- **No expectation of privacy:** The District reserves the right to monitor, inspect, log, or restrict any device, account, or activity on its network for safety, legal compliance, or operational needs.

4. Internet Safety & Filtering

In compliance with CIPA and Rhode Island law, BWRSD filters internet access to protect users.

- **Filtered categories include:**
 - Adult, explicit, or obscene content.
 - Illegal or dangerous material (drugs, weapons, self-harm, gambling, hate speech).
 - Distracting or unvetted tools (games, unmanaged social media, unverified search engines or AI tools).
 - Security risks (malware, phishing, hacking sites, proxy-bypass tools).
- **Administration:** Technology leadership manages filtering settings, which may vary by age or role. Exceptions can be made for legitimate instruction, research, accessibility, or operational needs.

5. Requesting to Unblock Websites

Teachers can request to unblock websites needed for instruction.

- Requests may be denied if the site poses security risks, violates privacy laws, or contains age-inappropriate content.
- Teachers will receive a specific reason for any denial and may appeal to the Superintendent.
- Consistent with R.I. Gen. Laws § 16-21.6-1, the District shall maintain a record of unblock requests and responses, report annually to the School Committee the number of requests granted and denied and review prior requests to determine whether filtering categories or procedures should be revised.

6. Violations & Consequences

Violations may lead to:

- Revoked technology privileges or device confiscation.
- Disciplinary action under student or employee conduct rules.
- Financial liability for equipment damages.
- Referral to law enforcement when appropriate.

7. Oversight, Emergency Response, & Training

- **Administrative Authority:** The Superintendent and Technology Directors set technical standards, security practices, and user requirements.
- **Emergency Action:** District IT staff may take immediate steps (such as disabling accounts or isolating devices) to stop active cybersecurity threats or data breaches.
- **Training:** BWRSD will provide regular instruction on digital citizenship, online safety, and security best practices.

Policy History & References

- **Consolidation:** Replaces prior versions of **JFB** (2018), **IIA**, and **GCQB**.
- **Cross-References:** JFBC, JFBC-E, EHAA, IJNDB.
- **Legal References:** CIPA (47 U.S.C. § 254), R.I. Gen. Laws § 16-21.6-1, R.I. Gen. Laws ch. 38-2 (APRA).

Adopted June 27, 2016

Revised September 14, 2026