Instruction

Information Technology Standards and Compliance Procedures

The Bridgeport Public School networks and services are provided as a service of the Bridgeport Board of Education for the purposes of academic and administrative needs. All users must comply with the District Policy 6401and adhere to the below standards for compliancy and enforcement thereof.

TECHNOLOGY STANDARDS

- **Microsoft Office 365** is the District standard platform for Students, Faculty and Staff for:
  - E-mail Services (*Outlook*)
  - Personal Work Document Storage (*OneDrive*)
  - Group Shared Document Storage (*SharePoint*)
  - Collaboration Services (*Teams*)
  - Student Learning Management System (*Teams for Classrooms*)
  - District Video Streaming Storage (*Stream*)
- **PowerSchool** is the designated District Student Information System for:
  - District Rostering
  - Classroom Management
  - Classroom Scheduling
  - Grades
  - All unspecified academic and administrative needs with the exception of IEP/504 management which is provided through Frontline IEP Direct
- **All District owned devices** must be enrolled in a District supported device management platform or mobile device management platform and include:
  - Microsoft Windows 7-10 (Active Directory)
  - Microsoft Windows 10S (Intune)
  - Apple Macintosh OS X (JAMF/Intune)
  - Apple IOS/iPadOS (JAMF/Intune)
  - Google ChromeOS (Google Enterprise)
  - Google Android OS (Intune)
- **Only District owned and Information Technology Services authorized computers** may be plugged into the District's wired ethernet network. Personal devices are not allowed unless special ITS exemption is made. This includes but is not limited to personally owned:
  - Computers, Laptops, Micro-devices, IoT Devices
  - Cameras
  - Switches
  - Access Points and Routers
  - Storage Systems
- **District Wireless Networks** must be used in accordance with Policy 6401 and must be used in the following manner per SSID (Network Name):
  - **Wireless:** Used for all District owned faculty and staff owned devices
  - **BBOEWireless-DistrictDevices**: All District owned student devices
  - **BBOEWireless-Displays:** All District owned projectors, presentations devices
  - **BBOEWireless-BYOD:** All personally owned devices for students, faculty and staff
  - **BBOEWireless-Guest:** All non-affiliated visitors to Bridgeport Public Schools

ITS Technology Compliance (continued)

SOFTWARE STANDARDS

All unauthorized software is forbidden to be installed on District owned computers that has not been expressly approved for usage through the state of Connecticut PA-16-189 Compliance Policy and the department of Information Technology Services.

- **Specific examples of unapproved software** may include but is not limited to:
  - Virtual Private Network clients/servers (OpenVPN, IPSEC, PPTP, etc)
  - Reverse Tunneling VPN Software (Hamachi, SSH, etc)
  - Firewall penetrating Remote Desktop (Goto My PC, Chrome Remote Desktop, etc)
  - VPN Tunneling software for the purposes of bypassing District security protocols and safeguards
  - WiFi Tunneling (NordVPN, etc)
  - Unauthorized DNS Servers (Google DNS, OpenDNS, etc)
  - Anonymizer Clients (HTTP/HTTPS Clients)
  - Proxy Software and relay software (HTTP/HTTPS bypass)
  - Network Address Translation bypass software (DNS Tunneling, UDP Tunneling)
  - The Onion Router Clients (ToR)
  - Hacking software
  - Keylogging software