NonDPS Device Network Policy

1. Overview

DPS provides a guest network for users of nonDPS owned devices to access the Internet that complies with mandates of the Children's Internet Protection Act (CIPA). This policy outlines the requirements for devices not owned by DPS using the DPS network may only connect the DPS guest network.

2. Purpose

This policy for Acceptable Use of nonDPS owned devices on the DPS guest network is to is to prevent unauthorized use, access and other unlawful activities by users online and offline, prevent unauthorized disclosure of or access to District information, and to comply with the Children's Internet Protection Act ("CIPA") including without limitation, all applicable state and federal laws concerning electronic communications, privacy, copyrights, personally identifiable, confidential, and legally protected information.

3. Scope

This policy applies to all users of the DPS internet with nonDPS owned computers or devices.

4. Policy

A computer or other device that is not owned by DPS ("nonDPS Owned") may only be connected to the DPS guest network. NonDPS Owned devices may not be connected to DPS' other networks including wired, staff or student wireless networks.

4.1 General Use

4.1.1 All users of DPS networks and internet must comply with DPS School Board policies and regulations.

4.1.2 DPS does not support nonDPS owned devices nor the installation of any District-supported software or applications on nonDPS owned devices.

4.1.3 Use of DPS networks constitutes consent to monitoring. During monitoring, any available information may be examined, recorded, and copied to protect against unauthorized use and preserve the stability of the system. Evidence of any unauthorized use collected in monitoring may be used for administrative, criminal, or other adverse action.

4.1.4 Users of nonDPS Owned devices who require access to data and systems internal to the DPS Network must comply with the DPS Remote Access policy.

5. Policy Compliance

5.1 Compliance Measurement

The DoTS InfoSecurity Team will verify compliance to this policy through various methods, including but not limited to, network monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate Principal or Executive Director.

5.2 Exceptions

Any exception to the policy must be approved by the DoTS InfoSecurity Team in advance.

5.3 Non-Compliance

An Authorized User found to have violated this policy may be subject to disciplinary action, up to and including termination of access or employment.

6. Policy Compliance

- Board Policy EGAEA – Electronic Mail and Internet Policy
- Board Policy EGAEA-R1 – Regulation of use of Electronic Mail and Internet
- Board Policy EGAEA-R2 – Regulation of Social Media

7. Policy Compliance

Date of Change	Responsible	Summary of Change
March 2019	Robert Losinski, Manager of Information Security	Creation.