Date Adopted: 05/09/2011	File Number: Detroit Lakes Policy - 552
Date Revised:	

552 – WIRELESS NETWORK POLICY

Overview

The purpose of this policy is to explain the Detroit Lakes Public Schools (District) standards, conditions, and requirements under which access is granted to the District's wireless network. This policy also strives to secure and protect the information assets owned by the District. The District provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. The District grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless capable devices (hereafter referred to as "wireless devices") must satisfy to connect to the District network. Only those wireless devices that meet the standards specified in this policy shall be allowed connectivity to the District network.

This policy works in conjunction with the District's Acceptable Use Policy. All Internet access via all (private and public) District wireless networks shall adhere to CIPA regulations. All persons connecting to any District wireless network must agree to the Wireless Communication Policy and the Acceptable Use Policy (presented via the captive portal screen).

Scope

All persons that connect to the District network via a wireless device must adhere to this policy. This policy applies to all wireless devices that connect to the District network or reside on a District site that provide wireless connectivity to endpoint devices including, but not limited to, notebooks, desktops, cellular phones, wireless enabled devices, and personal digital assistants (PDA's). This includes any form of wireless communication device capable of transmitting packet data.

Policy Statement

The District's wireless network is divided into two major components, a "Public" side and a "Private" side. ***The District reserves the right to regulate and control the level of access that is provided to users of either the "Public" Side or "Private" Side of the wireless network.*** Listed below is information regarding access to each.

Public Wireless Network Access

Employees of the District and persons not employed by the District ***including students*** shall be allowed connectivity to the District's public wireless network. District owned and non District owned wireless devices shall be allowed connectivity to the District's public

wireless network. Use of the public network implies no guarantee for quality of service or availability of service.

Private Wireless Network Access

Employees of the District or other persons approved by the Superintendent or his***/her*** designee shall be allowed access to the District's private wireless network. Wireless devices owned by the District or those devices approved by the Superintendent or his***/her*** designee shall be allowed access to the District's private wireless network. In order to gain access to the private wireless network, all of the aforementioned wireless devices must meet District standards: The District standards can be found at:
http://www.rschooltoday.com/se3bin/clientschool.cgi.

Liability

To the extent permissible by law the District hereby excludes all liability in tort (including negligence), contract or otherwise for any claim, loss, demands or damages of any kind whatsoever (whether such claims, losses, demands or damages were foreseeable, known or otherwise) arising out of or in connection with any usage of the wireless network or the information, content or materials included on/in the wireless network, including without limitation, indirect or consequential loss or damage; loss of reputation; or loss of damage to or corruption or disclosure of data or material.

Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with the District. ***A violation of this policy by a student may result in disciplinary action as determined by the principal and will be in accordance with the District's Student Policy Provisions.***

Anyone found to have violated this policy my be subject to disciplinary action, up to and including Police involvement and banned from Detroit Lakes Public School's buildings and activities.

Definitions

Term	Definition
Detroit Lakes Public School's network	A wired or wireless network including indoor and outdoor networks that provide connectivity to District services.
Information assets	Information that is collected or produced and the underlying hardware, software, services, systems, and technology that is necessary for obtaining, storing, using, and securing that information which is recognized as important and valuable to the District.

MAC address	The MAC address is a hardware number that uniquely identifies each node on a network and is required for every port or device that connects to the network.
Packet Data	Information that is reduced into digital pieces or 'packets', so it can travel more efficiently across networks, including radio airwaves and wireless networks.
Captive Portal	A Web page that the user of a public-access network is obliged to view for authentication purposes before access is granted.
Private wireless network	A network that provides access to the District's confidential information assets.
Public wireless network	A network that provides guests web access only.
CIPA	Children's Internet Protection Act is a federal law enacted by congress to address concerns about access to offensive content over the Internet on all District computers.