Deer/Mt Judea School District

Wireless Acceptable Use Policy (Student)

2015-2016

1.0 Purpose

This policy prohibits access to networks via unsecured wireless communication devices. Only wireless systems/devices that meet the criteria of this policy or have been granted access by the Technology Coordinator are approved for connectivity to Deer/Mt Judea School District's Wireless network. The purpose of this policy is to protect our District from unauthorized use and/or malicious attacks that could result in the loss of data, damage to critical applications/equipment, or damage to our public image.

2.0 Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, tablets, PDAs, etc.) connected to any of Deer/Mt Judea School District's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Deer/Mt Judea School District's networks do not fall under the purview of this policy.

3.0 Policy

3.1 Agreement

By connecting to the Deer/Mt Judea School District Wireless Network, You agree to follow the rules and regulations stated in the Acceptable Use Internet Agreement. The Deer/Mt Judea Technology Department reserves the right to turn off, without notice, any device connected to the network that it feels puts the district's systems, data and users at risk. Any device or equipment found to be interfering with access point signals may be subject to relocation or removal. Users are expected to secure their devices when they are physically at their machines as well as when they are away from their machine.

3.2 Register Access Points and Cards

All wireless Access Points connected to the Deer/Mt Judea School District's Networks must be approved by the Technology Coordinator. These Access Points are centrally managed by the Technology Coordinator and are subject to periodic penetration tests and audits. All wireless

Network Interface Cards (i.e., PC cards) used in District laptops or desktop computers must be approved before use.

3.3 Authentication

For a user to connect to the Deer/Mt Judea Wireless Network, one must obtain the WPA key from Authorized Personnel. Users knowingly or negligently allowing unauthorized access will face disciplinary action.

3.4 Setting the SSID

The SSID shall be configured so that it does not contain any identifying information about the organization, such as the district name, division title, employee name, or product identifier.

4.0 Enforcement

Any Wireless User in violation of the Deer/Mt Judea School District's Wireless Access Policy may result in suspension of wireless access privileges and possible disciplinary action.

Student Signature: ______________________________ Date: ____________

Parent Signature: ______________________________ Date: ____________