Internet Connection Policy

1.0 Overview

This internet connection policy requires users to use the internet for educational purposes only and requires users to avoid going to malicious web sites which could compromise security. It informs the users that their internet activity may be logged and monitored and defines whether user activity on the network will be logged and to what extent. It specifies what system will be used to prevent unauthorized viewing of sites and what system will log internet usage activity. This policy defines whether a proxy server will be used for user internet access. It defines how the network will be protected to prevent users from going to malicious web sites.

2.0 Purpose

This policy is designed to protect the organizational resources against intrusion by malware that may be brought into the network by users as they use the internet. It is also designed to prevent unauthorized and unprotected connections to the internet which may allow a host of unsafe content to enter the organizational network and compromise data integrity and system security across the entire network.

3.0 Scope

This internet connection policy applies to all users.

4.0 Physical Internet Connection

All physical internet connections or connections to other private networks shall be authorized and approved by the IT department. No FAX, modem, or digital lines will be authorized or installed for personal use. Most users will access the internet through the connection provided for their office by the IT department. Any additional connections must be approved by the IT department. These additional connections include but are not limited to:

1. Modem connection from a computer or communication device which may allow a connection to the network.
2. Any multipurpose printing and FAX machines which have both a phone and network connection must be examined and approved for use by the IT department.
3. Wireless access points or devices with wireless capability are allowed unless blocked by the IT department.
4. Any electronic connection to a device connected to the internal network.
5. FAX lines

Any additional internet connections not provided by the IT department must be reviewed and approved by the IT department. Typically any additional connections from the organizational network to the internet or other private network will require:

1. An IT department approved firewall operating at all times and properly configured.

2. Some communications through the connection may require encryption subject to a review of data to be transmitted by the IT department.

5.0 Use of the Internet

1. All employee and student use of the internet shall be for educational purposes only.
2. Employee and student use of the internet may be monitored and logged including all sites visited, the duration of the visits, amount of data downloaded, and types of data downloaded. The time of recorded activity may also be logged.
3. Employees and students are urged to use caution when visiting unknown internet sites and through user training set and keep their browser configured to IT approved standards in order to protect against infections of malware.

6.0 Internet Control and Logging System

A system will be required to operate on the network with the following capabilities:

1. The ability to prevent users from visiting inappropriate, pornographic, or dangerous web sites. It will have its database of categorized websites updated regularly.
2. The ability to log user internet activity including:
    1. Time of the internet activity.
    2. Duration of the activity.
    3. The website visited.
    4. Data and type of data downloaded
3. The system will not require a login ID or it will use the current network login to identify users.

The system used to prevent users from visiting inappropriate, pornographic, or dangerous web sites shall be Lightspeed Systems. This same system will not require an additional login ID and will use Active Directory and Google Login to identify internet users. The system shall be able to log the time of internet activity, duration of the activity, the website visited, any data downloaded and the type of data downloaded. The Appliansys Cachebox system will cache web pages.

7.0 Enforcement

Since improper use of the internet or use of unauthorized connections to the internet or other networks may compromise network security, destroy the integrity of network resources and systems and the prevention of these events is critical to the security of the organization and all individuals, employees and students that do not adhere to this policy may be subject to an account lock.

8.0 Additional Information

The Orchard Farm School District provides an Internet connection for district faculty, staff, and students to use for approved services. The Internet connection at the Orchard Farm School District is provided by two ISP's in a spillover configuration by The New Florence Telephone Company and MOREnet Communications. Windstream provides an additional Internet connection for the telephone system at Discovery Elementary.

The Orchard Farm School District does not support faculty, staff, or student owned personal hotspots. If the technology department suspects that a device may be interfering with the district's network configuration the device may be blocked or disabled.

The district's Internet is filtered using Lightspeed Communications Internet filter in conjunction with Dell Sonicwall's Internet filter. The Lightspeed Rocket appliance is used to set policies, block and unblock websites using the appliance's dashboard. The Lightspeed Rocket is also configured to provide off-site Internet filtering for students using district owned Chromebook devices and district Google Apps for Education accounts. The Dell Sonicwall is configured with Internet filtering to block websites in the event the Lightspeed Rocket fails to block an inappropriate website. The Dell Sonicwall also blocks proxy attempts that have not been properly allowed through the firewall.

The technology department also implements an Appliansys Cachebox appliance to conserve Internet bandwidth.This appliance provides some reporting and a whitelist to bypass caching of specified websites.

For wireless connections the district has created an OFSD ssid for district owned devices to connect and gain network and Internet access. This ssid is secured using a WPA2 passphrase. The district also has the OFSDpublic ssid for public Internet access. There are no security requirements to join this ssid and users must acknowledge our connection page to continue to the Internet. Users connected to OFSDpublic will also be filtered by the Lightspeed Rocket appliance.

LAST PRINTED 6/2/16