

# Monitoring and Filtering Internet Use

## I. Purpose

The purpose of this policy is to define standards for systems that monitor and limit Internet use from any device within Dyersburg State Community College's (DSCC) network. These standards are designed to ensure employees and students use the Internet in a safe and responsible manner, and ensure that employee web use can be monitored or researched during an incident.

## II. Scope

This policy applies to all DSCC employees, students, contractors, vendors and agents using a DSCC-owned or personally-owned computer or workstation connected to the DSCC network. This policy also applies to all end-user initiated communications between DSCC's network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols.

## III. Policy

### Web Site Monitoring

The Information Technology Department shall reserve the right to monitor Internet use from all computers and devices connected to the corporate network. For example, monitoring may be done to investigate system problems or at the request of an employee's supervisor. The Vice President for Information Technology and Facilities Management must be informed by the IT staff of any needed monitoring situation.

### Access to Web Site Monitoring Reports

General trending and activity reports will be used as necessary for troubleshooting and planning purposes. Internet Use reports that identify specific users, sites, teams, or devices will only be made available outside the IT department upon written or email request to the Vice President for Information Technology and Facilities Management from Human Resources and/or a member of the President's Cabinet.

### Internet Use Filtering System

The Information Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for DSCC's environment. The following general categories of websites should be blocked:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Gambling
- Hacking
- Illegal Drugs
- Peer to Peer File Sharing
- Personals and Dating
- Spam, Phishing and Fraud

- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate

### **Internet Use Filtering Rule Changes**

The Information Technology Department shall periodically review and recommend changes to web and protocol filtering rules to the Vice President for Information Technology and Facilities Management. Any changes to web and protocol filtering rules will be recorded in this policy.

### **Internet Use Filtering Exceptions**

If a site is incorrectly categorized, employees may request the site be un-blocked by submitting a request to the Vice President for Information Technology and Facilities Management. The Vice President for Information Technology and Facilities Management will work with the employee and other IT staff to determine whether it should be unblocked.

Employees may access blocked sites with permission if appropriate and necessary for business or educational purposes.

## **IV. Compliance**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any student found to have violated this policy may be subject to disciplinary action, up to and including suspension.

## **V. Definitions**

**Internet Filtering** The use of technology that monitors each instance of communication between devices on the college network and the Internet and that blocks traffic matching specific rules.

**Peer to Peer File Sharing** Services or protocols such as BitTorrent that allow Internet connected hosts to make files available to or download files from other hosts.

**Spam** Unsolicited Internet Email. Spam sites are websites link to from unsolicited Internet mail messages.

**Phishing** Attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication.

**Hacking** Breaking or subverting computer security controls.

## **VI. Revision History**

Policy written April, 2011 by Vice President of Technology; approved by Administrative Council on 04/29/2011.

Policy revised June, 2011; approved by Administrative Council on 06/21/2011.

Policy revised 4/22/2024; approved by Administrative Council on 04/25/2024.