Catholic Diocese of Columbus

Employee Internet Use, Monitoring and Filtering Policy

Steve Nasdeo

Diocesan Director of Technical Services and Catholic Schools

June 2017

Table of Contents

1. Overview 3
2. Purpose 3
3. Scope 3
4. Policy 3
5. Policy Compliance 4
5.2 Exceptions 4
5.3 Non-Compliance 5
6 Related Standards, Policies and Processes 5
7 Definitions and Terms 5

Revision History

Date of Change	Responsible for Change	Change Summary
15 June 2017	Steve Nasdeo	Initial Policy Document
25 June 2019	Steve Nasdeo	Changes to blocked categories

Employee Internet Use, Monitoring and Filtering Policy

1. Overview

See Purpose.

2. Purpose

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within the Catholic Diocese of Columbus's network. These standards are designed to ensure employees use the Internet in a safe and responsible manner and ensure that employee web use can be monitored or researched during an incident.

3. Scope

This policy applies to all Catholic Diocese of Columbus employees, contractors, vendors and agents with a Catholic Diocese of Columbus-owned or personally-owned computer or workstation connected to the Catholic Diocese of Columbus network.

This policy applies to all end user-initiated communications between Catholic Diocese of Columbus's network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

4. Policy

4.1 Web Site Monitoring

The Technical Services Department shall monitor Internet use from all computers and devices connected to the diocesan network. For all traffic, the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for 180 days.

4.2 Access to Web Site Monitoring Reports

General trending and activity reports will be made available to any department as needed upon request to the Director of Technical Services. The Office of Technical Services' Computer Security Incident Response Team (CSIRT) members may access all reports and data if necessary, to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the CSIRT upon written or email request to the Director of Technical Services from a Human Resources Representative and with an active Confidential Investigation opened.

4.3 Internet Use Filtering System

The Technical Services Department shall block access to Internet websites and protocols that are deemed inappropriate for the Catholic Diocese of Columbus's environment. The following protocols and categories of websites, will be blocked unless an approved exception is allowed:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups (to the extent possible)

- Chat and Instant Messaging (outside of Microsoft Teams)
- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing
- Personals and Dating
- Social Network Services (see Social Media Acceptance Policy)
- SPAM, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate

4.4 Internet Use Filtering Rule Changes
The Office of Technical Services shall periodically review and recommend changes to web and protocol filtering rules. The IT Steering Committee shall review these recommendations and decide if any changes are to be made. Changes to web and protocol filtering rules will be recorded in the Internet Use Monitoring and Filtering Policy.

4.5 Internet Use Filtering Exceptions
If a site is mis-categorized, employees may request the site be un-blocked by submitting a ticket to the Technical Services help desk. The Director of Technical Services will review the request and un-block the site if it is mis-categorized.

Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to the Office of Technical Services via either a helpdesk ticket or by calling the helpdesk. The Director of Technical Services or their delegate, will investigate the request. If the request is approved, the technician will unblock that site or category for that associate only. Office of Technical Services will track approved exceptions and report on them upon request.

5. Policy Compliance

5.1 Compliance Measurement
The Office of Technical Services team will verify compliance to this policy through various methods, including but not limited to, periodic walk-arounds, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions
Any exception to the policy must be approved by the Director of the Office of Technical Services in advance.

5.3 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

None.

7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Peer to Peer File Sharing
- Social Networking Services
- SPAM
- Phishing
- Hacking