Catholic Diocese of Columbus

Removable Media Policy

Steve Nasdeo

Diocesan Director of Technical Services and Catholic Schools

September 2018

Table of Contents

Revision History

Date of Change	Responsible for Change	Change Summary
14 June 2017	Steve Nasdeo	Initial Policy Document
17 Sept 18	Steve Nasdeo	Final policy wording
20 Sept 18	Steve Nasdeo	Policy Approved – marked FINAL

Removable Media Policy

1. Overview

Removable media is a well-known source of malicious code (malware) infections and has been directly tied to the loss of sensitive information in many organizations.

2. Purpose

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by the Catholic Diocese of Columbus and to reduce the risk of acquiring any infections on computers operated by the Catholic Diocese of Columbus.

3. Scope

This policy covers all diocesan owned computers (laptops and desktops) and servers operating on the Catholic Diocese of Columbus network, connected either directly (wired) or wireless.

4. Policy

- The use of removable media on diocesan owned computers by the Catholic Diocese of Columbus staff is not allowed.
- We will disable, via group policy, all USB ports used for storage devices on all Catholic Diocese of Columbus owned, leased or operated equipment.
- Computers not owned or leased by the Catholic Diocese of Columbus may not use removable media without explicit permission of the Director of Technical Services or their delegate.
- Sensitive information should only be stored on removable media when required in the performance of your assigned duties or when providing information required by state or federal agencies.
    - A policy waiver must be on file to have access to the data.
- If sensitive information is permitted to be stored on removable media, it must be encrypted in accordance with the Catholic Diocese of Columbus *Acceptable Encryption Policy*.
    - An approve policy waiver must be on file with the Office of Technical Services
    - Once the removable media is encrypted, you will be provided with a password for access to the data on that device
    - You are responsible for safely storing and the use of this password.

Exceptions to this policy may be granted on a case-by-case basis by contacting the Technical Services helpdesk or the Director of the Office of Technical Services.

5. Policy Compliance

5.1 Compliance Measurement

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

5.2 Exceptions
The Director of Technical Services or their delegate must approve any exception to this policy 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. Any non-employee found to have violated this policy will be subject to being blocked from further use of any diocesan owned network.

6 Related Standards, Policies and Processes

- Acceptable Encryption Policy

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/

- Encryption
- Malicious Code
- Malware
- Removable Media
- Sensitive Information