Anti-Malware Policy

© William College. All rights reserved

Document Version Control	
Document Title:	Anti-Malware Policy
Version:	1.0
Approving Committee:	Senior Leadership and Management Team
Policy Lead:	IT Coordinator
Date of Last Review:	April 2026
Date of Approval:	May 2026
Date Effective from:	June 2026
Date of Next Review:	November 2027

© William College. All rights reserved

Table of Contents

1. Introduction 3
2. Coverage 3
3. Policy Specifications 3
4. Roles & Responsibilities 3
   4.1 All Staff and Contractors 3
   4.2 IT Team 4
5. Policy Review 4
6. Related Policies and Docuements 4

© William College. All rights reserved

1. Introduction

This policy has been deliberately designed to protect the confidentiality, integrity, and availability of our information resources. It presents a systematic method for identifying, preventing, and resolving risks associated with computer viruses and harmful software that could threaten our systems and data.

2. Coverage

This policy is applicable to staff and contractor usage of all information systems within William College, including those accessed through standard network links or VPNs, as well as personal devices governed by the Bring Your Own Device (BYOD) Policy. Deliberate approaches of overcoming or deactivating security measures set up by the institution will be treated as a disciplinary case under the Staff Disciplinary Policy. Detected cybersecurity breaches are to be reported to the IT team immediately.

This policy is part of the measures William College takes to ensure IT security and should be read in conjunction with the Acceptable Use of IT Services Policy, Password Management Policy, Access Control Policy and Web Filtering & Monitoring Policy.

3. Policy Specifications

To maintain the security and robustness of William College's systems, the following baseline requirements must be upheld without exception:

- Anti-virus software approved by the IT team with valid licenses must be installed on every workstation and virtual system connected to the network.
- Real-time anti-virus protection must be enabled on all servers and client devices.
- Virus definition databases must be refreshed daily, with automatic updates turned on.
- Devices found to be infected must be disconnected from the network immediately until they are confirmed to be clean.
- Antivirus scans must cover executable files (including macro-enabled data files), all data files including compressed or password-protected ones, removable media, and web pages as they are accessed. Any files not scanned must be recorded.
- Systems must be set up to automatically scan removable media upon connection.
- Alerts must be activated when a virus is suspected.
- All user-managed servers and workstations must undergo weekly virus scans.

4. Roles & Responsibilities

4.1 All Staff and Contractors

Any potential sign of computer virus (such as sluggish performance or unusual files) must be notified to IT staff right away and the device disconnected from the network.

- Alteration or disabling of anti-virus settings can only be done by a member of the IT Team and have received approval from senior leadership.
- Files originating from external or unverified sources must be scanned before use.
- It is strictly not allowed to create or spread malicious software.

© William College. All rights reserved

4.2 IT Team

- Ensure enforcement and oversight of this policy.
- Offer support for installation and provide best practice advice for virus protection.
- Help with virus detection, containment, and resolution.

5. Policy Review

This policy is reviewed every eighteen months by the Senior Leadership and Management Team and may be triggered by legislative changes.

6. Related Policies and Documents

- Acceptable Use of IT Policy
- Staff Bring Your Own Device (BYOD) Policy
- Data Breach Management Procedures
- Starters and Leaver Checklist
- Staff Disciplinary Policy

© William College. All rights reserved