Anti-Malware Policy

Full Council Approved:	3 June 2026
Last Reviewed:	June 2026
Due for next Review:	June 2029

1. Purpose

The purpose of this policy is to ensure the confidentiality, integrity, and availability of information in a clear and consistent structure. It will rely on detection, prevention, and correction against computer viruses and/or malicious software that could otherwise cause significant damage to information and information resources.

2. Scope

The scope of this policy applies to all Fleet Town Council information systems and those that are connected to the network via standard network connection or a Virtual Private Network (VPN).

3. Policy

This policy is designed to protect Fleet Town Council's resources against intrusion, modification, and destruction of information by viruses and other malware. The following minimum requirements must remain in force until further notice:

- All workstations attached to Fleet Town Council network must have licensed anti-virus software installed from approved vendors for anti-virus protection. This also includes the virtual environments.
- The anti-virus product must be operated in real time and be always active on all servers and client computers.
- The anti-virus library definitions must be updated at least once per day and set as automatic update.
- The anti-virus scans must be done a minimum of once per week on all user-controlled workstations and servers.
- The antivirus scans must include but not limited to:
- All executable files (including macros contained in data files).
- Data files including protected files (e.g., compressed or password protected files).
- Removable storage media.
- Any files that have not been scanned for any reason must be logged in the anti-virus log history.
- Webpages as and when they are visited
- The anti-virus product must provide an alert when a suspected virus has been detected.

- Virus-infected computers must be removed from the network until they have been verified as virus-free.
- All systems must be configured to perform an automated anti-virus scan of removable media when it is inserted.

4. Roles and Responsibilities

Councillors, Employees or Others Working for Fleet Town Council

- If a file is received that is what is believed to be a virus, or there is suspicion that a computer is infected with a virus, such as due to a performance slowdown, this must be reported to the Executive Officer immediately and the device removed from Fleet Town Council's network.
- Anti-virus definition updates, scans or core functionality should never be tampered with or disabled except from the members of the IT Support (Cloudy IT) and only with Executive Officer approval.
- Any files from external sources, uncertain or unauthorised sources or over non-trusted networks, must be checked for malware before use.
- Fleet Town Council prohibit any activity intended to create and/or distribute malicious code on the Fleet Town Council network or IT facilities.

IT Support

- Ensure the compliance and enforcement of this policy.
- Provide advice to individuals on installing the antivirus products and on virus protection in general.
- Assist individuals with recovery from viruses.

5. Related Documents

- Access Control Procedure
- Acceptable Use Policy
- Information Security Awareness Policy
- Password Policy