



# Information Security Awareness 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 provide all Councillors and employees, including contractors with the required knowledge and best practices. To ensure that everyone is aware of their role in safeguarding the confidentiality, integrity and availability of Council data, services, and systems. To encourage ultimately a formal security culture.

## 2. Scope

This policy applies to Councillors and employees that use or manage Council systems including those that are temporary contracted. This extends to all administrative staff in all levels.

## 3. Policy

- All new Councillors and employees must complete an approved Security Awareness training prior to, or within 30 days of, being granted access to any Fleet Town Council information resources.
- All information security policies must be made openly available to all Councillors and staff. To allow them to properly protect Fleet Town Council information resources.
- Councillors and staff are required to acknowledge that they have agreed, received, and will adhere to the Fleet Town Council information security policies before they are granted access to the Fleet Town Council sensitive information resources.
- All Councillors and employees must complete an annual security awareness training.
- There must be evidence and record of all security awareness training delivered.
- Fleet Town Council's IT Support supplier must develop and maintain a process to be able to communicate new security program information, security bulletin information and security items of interest.
- 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. Enforcement**

Users shall abide to existing information security policies and procedures. Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or contract or agreement.

#### **5. Related Documents**

- Access Control Procedure
- Acceptable Use Policy
- Anti-Malware Policy
- Password Policy