Computer Use and Communications Policy

Policy and Finance Approved:	January 2015
Reviewed:	February 2025
Due for Review:	February 2028

1 Introduction

To provide our employees with the tools to do their jobs, Fleet Town Council makes available to its workforce access to one or more forms of electronic equipment and software, including computers, e-mail, telephones, and internet.

All employees and everyone connected with the Council should remember that electronic equipment and software provided remain the Councils property. All computer users have the responsibility to use these resources in a professional, ethical, and lawful manner.

2 Purpose of this Policy

To ensure that all employees are responsible for following guidelines which have been established for using computers, e-mail, telephones, internet or other software. No policy can lay down rules to cover every possible situation. Instead, it is designed to express the Council's philosophy and general principles when using electronic media when communicating both internally and externally on behalf of Fleet Town Council.

3 Prohibited Communications

Written and electronic media cannot be used for knowingly transmitting, retrieving, or storing any communication that is:

- Discriminatory or harassing;
- Derogatory to any individual or group;
- Obscene, sexually explicit or pornographic;
- Defamatory or threatening;
- In violation of any license governing the use of software; or
- Engaged in for any purpose that is illegal or contrary to Fleet Town Council policies or business interests.

Adopted by P&F Committee – 19 January 2015
Reviewed – October 2018; October 2021, February 2025

4 Personal Use

The computers, electronic media and services provided by the Council are primarily for business use to assist employees in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not impact on individual's performing their jobs or negatively affect the systems' use for their business purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

5 Access to employee communications

The Council reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other policies.

Employees should not assume electronic communications are private. Accordingly, if they have sensitive information to transmit, they should use other means.

6 Software

To prevent computer viruses from being transmitted through the computer system, unauthorised downloading of any unauthorised software is strictly prohibited. Only software registered and/or approved through the Council may be downloaded. Employees should contact Cloudy IT, the Councils system administrator, if they have any questions.

7 Security/Appropriate Use

Employees must respect the confidentiality of other individuals' communications.

Employees are prohibited from engaging in, or attempting to engage in:

- Monitoring or intercepting the files or electronic communications of other employees or third parties;
- Using other people's logins or passwords;
- Except in cases in which explicit authorisation has been granted by management, no e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else; and
- All employees should be aware of the increasingly sophisticated scams and risks proposed to cybersecurity and when in any doubt should seek guidance from Cloudy IT.

8 Violations

Any employee who abuses the privilege of their access to e-mail or the Internet in violation of this policy may be subject to disciplinary action including possible termination of employment, and/or legal or criminal action.

Adopted by P&F Committee – 19 January 2015
Reviewed – October 2018; October 2021, February 2025

9 Training and Guidance

Employees will be provided with regular cybersecurity training, software training and other appropriate training for their role and level of systems access.

10 Passwords

All computers, including laptops and tablets will require 2 factor authentication, which is set up by Cloudy IT, the system administrator. If you do not have a work mobile, your personnel mobile number will be required for authentication.

Passwords and logins must not be shared.

11 Incident Reporting

All employees must report any incident which could pose a risk to the Councils systems or data security to the Executive Officer without delay. This includes but is not limited to:

- Lost devices
- Potential risk arising from phishing emails/websites
- Passwords having been shared or compromised
- Unauthorised access to systems.

Adopted by P&F Committee – 19 January 2015
Reviewed – October 2018; October 2021, February 2025