WTC INFORMATION SECURITY POLICY

1.   **INTRODUCTION**

In order to ensure smooth and efficient running of council affairs, Whitehill Town Council is making increasing use of Information and Communication Technology (ICT) and information held by the Council and other public-sector organisations.

The Council aims to ensure that personal information held is kept to a minimum and only where required for legitimate Council business. The Council needs to maintain public confidence by ensuring any information it processes, maintains and shares with other public-sector organisations is protected by appropriate levels of information security.

2.   **PURPOSE**

This document describes the Information Security Policies adopted by Whitehill Town Council. The objective of these policies is to ensure that appropriate standards of information security are maintained across the Council at all times so that:

- The public and all users of the Council's information systems are confident of the security, integrity and availability of the information used and produced
- Damage and interruption caused by security incidents are minimised
- All legislative and regulatory requirements are met
- The Council's equipment and facilities are used responsibly, securely and with integrity at all times.

The policy adopted by Whitehill Town Council are based on industry good practice and covers the following:

- Email Policy
- Internet Acceptable Usage Policy
- Software Policy
- IT Access Policy
- Information Protection Policy
- Computer, Telephone and Desk Use Policy
- Legal Responsibilities Policy
- Remote Working Policy
- Removable Media Policy
- Information Security Incident Management Policy
- Data Retention Policy

This document provides an overview of each of the individual policies, highlighting key messages that all members of staff need to be aware of when using electronic systems and sharing information with partner organisations.

All staff and councillors are required to sign this policy document to confirm:

- That they have read and understood these key messages.
- That they understand the consequences of failure to comply with these policies.
- That they understand they have a responsibility to familiarise themselves with the Information Security Policies listed in this document.

3. INFORMATION SECURITY POLICY DOCUMENTS

3.1 Email Policy

Policy Statement

Whitehill Town Council will ensure all users (councillors and staff) of Council email facilities are aware of the acceptable use of such facilities:

- Your personal e-mail address is your first name, followed by a full stop and then
- @whitehilltowncouncil.gov.uk e.g. first.last@ whitehilltowncouncil.gov.uk
- Users should not use non-work email accounts to conduct or support official Whitehill Town Council business.
- Under no circumstances should users communicate material (either internally or externally), which is defamatory, offensive or obscene.
- If you receive an email from a suspicious source or with an odd or unexpected subject title, you should treat it with suspicion and, if unsure how to proceed, refer to the Council's Data Protection Officer (DPO)
- An email has the same legal status as a paper document and may be disclosed under the GDPR or the Freedom of Information Act 2000. Further information on this can be obtained from the Data Protection Policy or by contacting the Council's DPO.
- All official external e-mail will carry the official Council disclaimer.
- Automatic forwarding of email is not permitted to prevent confidential material being forwarded inappropriately.

3.2 Internet Acceptable Usage Policy

Policy Statement

Whitehill Town Council will ensure all users of Council-provided internet facilities are aware of the acceptable use of such facilities:

- You must familiarise yourself with this policy and sign the policy before using the internet facility provided.

- Internet and email access is an important aide to productivity. Private Internet and e-mail usage by Council staff must be in personal time.
- You are responsible for ensuring the security of your email login identity and password. Do not disclose your password or share accounts with colleagues.
- Individual user login identity and passwords must only be used by that individual user, and they must be the only person who accesses their email account.
- Do not create, download, upload, display or access, sites that contain pornography or other material that might be deemed illegal, obscene or offensive.
- Users must assess any risks associated with internet usage and ensure that the internet is the most appropriate mechanism to use.

3.3 Software Policy

Policy Statement

Whitehill Town Council will ensure the acceptable use of software by all users of the Council's computer equipment or Information Systems.

- Under no circumstances should personal or unsolicited software be loaded onto a Council machine.
- Every piece of software is required to have a licence and the Council will not condone the use of any software that does not have a licence.

- You are not permitted to bring software from home (or any other external source) and load it onto Council equipment.
- Users must not attempt to disable or reconfigure the firewall or other security software on the Council's computer equipment.
- Illegal reproduction of software is subject to civil damages and criminal penalties.

3.4   IT Access Policy

Policy Statement

Whitehill Town Council will establish specific requirements for protecting information and information systems against unauthorised access.

Whitehill Town Council will effectively communicate the need for information and information system access control.

- When setting up your password, this must consist of 8 characters, a mixture of letters and numbers. At least one of the letters must be a capital letter, e.g. Monkey33.
- Passwords must be protected at all times.
- If you leave your desk, lock or log out from your computer.
- It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to the Council systems.
- Partner agencies or 3rd party suppliers must not be given details of how to access the Council's equipment without permission from the Council.

3.5   Information Protection Policy

Policy Statement

Whitehill Town Council will ensure the protection of all information within the custody of the Council

High standards of confidentiality, integrity and availability of information will be maintained at all times. Personal information will only be collected and processed when essential for Council business, and only for purposes defined and agreed in advance by the Council.

Personal information will only be collected and processed using procedures and systems defined and agreed in advance by the Council.

- Information is to be handled in accordance with the Retention Policy and destroyed appropriately.
- Where information is shared or disclosed, it should only be done so with approval from the DPO and Council.
- The Council must draw up and maintain inventories of all important information assets.

3.6   Computer, Telephone and Desk Use Policy

Policy Statement

Whitehill Town Council will ensure that users are aware of, and understand, the acceptable use of Whitehill Town Council's computer and telephony resources and the need to operate within a "clear desk" environment.

- Where possible, private telephone calls should be made outside standard hours.
- When you are driving on Council business, you must not answer a mobile phone, whether or not it is a hands-free set. Safely park the vehicle and turn off the engine before you answer or return the call.

- ICT equipment is provided for use on official business only.

3.7 Legal Responsibilities Policy

Policy Statement

This policy sets out the responsibilities of all staff under the GDPR and Freedom of Information Act 2000 and other relevant legislation.

- Personal data is data that relates to a living individual who can be identified.
- Individuals have the right to request access to their personal information held either in paper or electronic copy by the Council. The Council has 40 calendar days in which to supply this information.
- If you receive a request for information under the Data Protection Act, you should refer this request to the Council's DPO.
- The Freedom of Information Act 2000 allows access to records held by public authorities. If you receive a request for information under the Freedom of Information Act 2000, you should refer it to DPO who will co-ordinate a response.
- All Councillors and staff must accept responsibility for maintaining Information Security standards within the Council.

3.8 Remote Working Policy

Policy Statement

Councillors and staff (as approved by the Council) are required to work remotely in order to carry out Council business. Whitehill Town Council will ensure that all users who work remotely are aware of the acceptable use of portable computer devices and remote working opportunities.

- Do not email council information or documents to your private email address at home to work on.
- You may use your own home equipment when required for Council Business, but any Council data stored on the equipment should be appropriately managed in line with the Council's Data Retention Policy
- If you use a laptop or device provided by the Council it must not be used by other members of your family.
- You may not install or upgrade any software on a Council owned computer device.
- If you need to take confidential or sensitive information off-site, you must get authorisation from the Council. This should be avoided where at all possible.
- Care and attention must be taken to protect against damage, loss or theft, when transporting equipment and data between, the Council office, home, and remote locations.

3.9 Removable Media Policy

Policy Statement

Whitehill Town Council will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official Council business.

Removable media devices include:
- Memory stick/USB Keys
- Writeable CD/DVD
- Laptop
- Camera
- Memory Cards
- Floppy Disks

It is Whitehill Town Council policy to limit the use of removable media devices. The use of removable media devices will only be approved if it is required for Council business.

- All data stored on removable media devices must be assessed by the DPO and encrypted when required.

- Damaged or faulty removable media devices must not be used.
- If you receive a CD or memory stick from a third party, it must be virus checked using anti-virus software updated to current version prior to insertion in Council equipment.
- Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- Removable media devices that are no longer required, or have become damaged, they must be disposed of securely to avoid data leakage.

3.10   Information Security Incident Management Policy and Procedure

Policy Statement

Whitehill Town Council will ensure that it reacts appropriately to any actual or suspected incidents relating to information systems and information within the custody of the Council.

- If you lose or have a removable media device stolen, you must report this immediately to the DPO.
- If you suspect you have inadvertently emailed personal data to an incorrect recipient, you must report this immediately to the DPO.
- Any loss, or suspected loss of Council equipment must be reported immediately to the DPO.