WHITNASH TOWN COUNCIL

INFORMATION SECURITY POLICY

Policy Statement

Whitnash Town Council has a commitment to protect Council information.

- Information is a critical asset. All storage and transmission of information processed or controlled by Whitnash Town Council must only be carried out for the lawful purposes for which it is held.
- Information must be protected in a manner commensurate with its sensitivity, value, and criticality.
- Information must be protected from loss of confidentiality, integrity and availability.
- All personal information processed electronically or held in a structed manual filing system shall be processed in accordance with the Data Protection Act 1998. Utmost care must be taken when dealing with personal and sensitive information to ensure that it is never disclosed to anyone inside or outside the Council without proper authorisation.
- Information shall not be used in any way that might be seen as defamatory, libellous, insulting or offensive by others. Electronic and non-electronic communications shall not contain material that is profane, obscene, indecent, pornographic, defamatory, inflammatory, threatening, discriminatory, harassing (racially, sexually or otherwise offensive), subversive or violent, racist or of an extreme political nature, or which incites violence, hatred or any illegal activity.
- A process of continual review and improvement must be implemented.

Passwords and Authentication

- They must ALWAYS be used in conjunction with a Unique User ID.
- All system passwords are to be treated as ‘sensitive’ information.

Staff must not:

- Share system passwords with anyone, including peers, assistants or superiors.
- Discuss or talk about a password in front of others.
- Hint at the format of a password (e.g., "my family name").
- Reveal a password on any questionnaires.

- Share a password with family members.
- Reveal a system password to co-workers providing holiday or absence cover.
- Write passwords down.
- Store unencrypted passwords in a file on ANY computer system.
- Use the "Remember Password" feature of any applications.
- Never allow another person to login to the system with your login ID and password. This could result in you being responsible for the actions or another person.

Staff and Members must immediately change a password if they suspect that it has been compromised.

Password length must be a minimum of 8 characters.

Anti-Malware

- Staff must not disable anti-malware software running on, or prevent updates being applied to devices.
- The intentional introduction of viruses to Whitnash Town Council's computing infrastructure is strictly prohibited.
- Only software that has been authorised by Whitnash Town Council can be installed upon Whitnash Town Council's systems.
- Staff are responsible for immediately reporting any abnormal behaviour of the computing systems to the IT provider.
- Prior to any encryption, all files must be scanned for and cleaned of viruses before being sent to any third party.
- All Members and staff are responsible for ensuring that appropriate and effective anti-virus detection software is installed on the Town Council's IT system.

Preventing Malware attacks

- It is very important to keep Windows updated by ensuring Windows Update runs and updates are installed.
- Never open attachments you are not expecting.
- Never open ZIP files.
- Never open Word documents or Excel spreadsheets with Macros enabled.
- Ensure the cloud backup software is working.
- If something pops up on the screen that looks bad or says it is encrypting your files turn the power off at the socket immediately, don't shut the computer down normally and don't restart it.

Access Control

- Users must not allow anyone else to use their account, or use their computers while logged in with their account.
- Computer screens should be 'locked' or the user logged out before leaving any workstation or device unattended.
- Users should not leave workstations or devices in 'sleep mode' for convenience.

Clear Desk and Clear Screen

- No information should be left on a desk surface overnight or when the desk is unoccupied.
- Removable media and easily portable devices, such as laptop computers or iPads, that have not been physically secured, must not be left unattended on desks.
- Where lockable safes, filing cabinets, drawers, cupboards etc are not available, office / room doors must be locked if left unattended.
- At the end of each working day all sensitive information must be stored in locked furniture.
- All information, when printed, faxed or photocopied, is to be cleared from printers, faxes and photocopiers immediately and, when no longer required destroyed in a secure and reliable manner using approved methods.
- Computer screens should be ‘locked’ or the user logged out before leaving any workstation unattended, even for a brief period.
- Users should not leave workstations or devices in ‘sleep mode’ for convenience.

Preventing Malware attacks

- It is very important to keep Windows updated by ensuring Windows Update runs and updates are installed.
- Never open attachments you are not expecting.
- Never open ZIP files.
- Never open Word documents or Excel spreadsheets with Macros enabled.
- Ensure the cloud backup software is working.
- If something pops up on the screen that looks bad or says it is encrypting your files turn the power off at the socket immediately, don’t shut the computer down normally and don’t restart it.

Acceptable use of the internet

The use of the internet should be in accordance with the following guidelines:

- Transmission of any material in violation of any United Kingdom or other national laws is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws.
- Only access suitable material. Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Abide by copyright laws.
- Do not access Internet chat and social networking sites. These represent a significant threat to the network.
- Do not to attempt to download or install software from the Internet.
- Do not download or open file attachments unless you are certain of both their content and origin. File attachments may contain viruses or other forms of malware that may cause loss of data.