**HALEWOOD TOWN COUNCIL**

**I.T SECURITY POLICY 2021**

**Background**

Halewood Town Council recognises that it has a responsibility to ensure all sensitive data, information systems and all confidential material are protected from security threats and to mitigate risks that cannot be directly encountered. Halewood Town Council recognises that all users need to be aware of and understand their personal responsibilities to protect the confidentiality and integrity of the data that they access.

**Organisational Responsibilities**

Halewood Town Council will ensure that all users are aware of and can comply with this policy and other supporting policies, to safeguard the reputation and business of Halewood Town Council by ensuring its ability to meet our legal obligations and to protect us from liability or damage through misuse of our IT facilities.

**Data Protection**

• All laptops/desktops should be password locked prior to any employee leaving their desk unattended.

• Senior officers who hold confidential data must take particular care to ensure their devices are locked and inaccessible when they are not in the office.

• No employee should utilise or access any PC or laptop which belongs to an alternative user unless previously agreed. If a device is subsequently used inappropriately, you may be jointly responsible for any consequences that arise from such use.

• All sensitive data and knowledge should be saved securely and confidentially to the Halewood Town Council Teams site and, where necessary, restricted files should be password protected/encrypted.

• Any and all new user access to restricted folders on the Halewood Town Council Teams site must be requested, agreed and implemented via the Administration and Democratic Services Officer and/or the Town Manager.

**Asset Protection**

• Each employee should sign the relevant section of the Asset Register and, by doing so as outlined on the form, is taking full responsibility for the adequate care and protection of all kit for the duration of his/her employment with Halewood Town Council.

•Any inadequate care which exceeds reasonable wear and tear that may result in repair or replacement, and which is not covered via the council’s insurance, may be costed and deducted from your salary.

• All laptops/desktops must be locked, shut down and either taken home, or kept in a secure place overnight. They must be used for work purposes only and staff should take particular care to ensure the devices are not used to access inappropriate or illegal sites (whether by the individual staff member or, for example, a family member). Under no circumstances should an employee leave a council laptop or similar in a locked car (either overnight or at other times through the day).

• All equipment leant to you will be logged via specific serial numbers - any equipment change, return or allocation made for an existing employee must be recorded in the Asset Register and be signed off by the Administration and Democratic Services Officer and/or the Town Manager.

**Office Access**

• It is not advised for individual staff members to share fobs, should you temporarily not have access to your specific fob (for whatever reason) this must be logged with the Buildings and Safety Officer, and upon approval a temporary fob can be allocated in your name.

• It is pivotal that any fobs which are lost, stolen or misplaced are reported immediately to office management, your previous fob will be blocked and a new one will be issued.

**Linked Policies**

* Staff Code of Conduct
* Disciplinary Policy

|  |  |
| --- | --- |
| **Last Review Date** | July 2022 |
| **Next Review Date** | July 2024 |
| **Date Approved** | 12th July 2022 |
| **Review Cycle** | 2-yearly |