****

**Weaverham Parish Council**

**IT Security Policy**

**Introduction:**

This IT Security Policy outlines the guidelines and responsibilities for the appropriate use of IT resources by council members, employees, volunteers, and contractors. The aim is to protect the council's data, systems, and networks from security threats and ensure compliance with applicable laws and regulations.

**Scope:**

This policy applies to all individuals who use the parish council's IT resources, including computers, networks, software, devices, and data.

**Acceptable Use:**

1. IT resources are to be used for official council-related activities and tasks.
2. Personal use should be limited and should not interfere with council work responsibilities.
3. Users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

**Device and Software Usage:**

1. Authorised devices, software, and applications will be provided by the parish council for work-related tasks.
2. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited.

**Data Management and Security:**

1. All sensitive and confidential data should be stored and transmitted securely using approved methods.
2. Regular data backups should be performed to prevent data loss.
3. Secure data destruction methods should be used when necessary.

**Network and Internet Usage:**

1. Downloading and sharing copyrighted material without proper authorisation is prohibited.
2. Users should be cautious when opening email attachments or clicking on links to prevent phishing and malware threats.

**Password and Account Security:**

1. Users are responsible for maintaining the security of their accounts and passwords.
2. Passwords should be strong and not shared with others.
3. Regular password changes are encouraged to enhance security.

**Mobile Devices and Remote Work:**

1. Mobile devices provided by the parish council should be secured with passcodes and/or biometric authentication.
2. Remote work should be conducted using secure connections and approved devices.

**Reporting Security Incidents:**

1. All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation