WILPSHIRE PARISH COUNCIL

Wilpshire Parish Council recognised that data theft, scams and security breaches can have a detrimental impact on the council’s systems and cause business interruption. Wilpshire Parish Council has created this policy which outlines security measures put in place to protect its systems.

Purpose

The purpose of this policy is to:

1. Protect Wilpshire Parish Council’s data and infrastructure
2. Outline the protocols and guidelines that govern cyber security measures
3. Define the rules for council and personal use

Scope

This policy applies to all Wilpshire Parish Councillors,officers, contractors, volunteers, suppliers and/or any individuals with access at anytime to the Council’s electronic systems, information, software and/or hardware.

Confidential Data

Wilpshire Parish Council defines confidential data as:

1. Any unreleased and classified financial information
2. Any information spoken about in a meeting if a resolution has been made to exclude public and press
3. Customer. Supplier confidential information
4. Council contracts and legal records
5. Complainants personal data

Property and Device Security

1, Council Use

To ensure the security of all council-issued devices and information. Wilpshire Parish Council employees are required to:

A keep all council-issued devices or devices used for council business password protected [at least 8 characters]

B Do not share personal private passwords with colleagues, personal acquaintances and councillors.

C Regularly update devices with the latest security software

2. Personal Use

Wilpshire Parish Council recognises that employees may be required to use personal devices eg mobile phones or computer to access company systems.

Keep all devices password protected minimum8 characters

Install anti virus software and upgrade regularly

Use Secure and private networks

Email Security

Clerk to report any issues to the Council immediately

Be aware of phishing and other security issues

Date approved: March 2023