Appleton Parish Council

Appleton Parish Hall, Dudlow Green Road, Appleton, WA4 5EQ

Telephone 01925 268153 Email clerk@appletonpc.org.uk

Cyber-security Policy

Adopted on 15th December 2020

Introduction

The risk of data theft, scams, and security breaches can have a detrimental impact on a company's systems, technology infrastructure, and reputation. As a result, Appleton Parish Council has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

Purpose

The purpose of this policy is to (a) protect Appleton Parish Council's data and infrastructure, (b) outline the protocols and guidelines that govern cyber security measures, (c) define the rules for company and personal use, and (d) list the company's disciplinary process for policy violations.

Scope

This policy applies to all of Appleton Parish Council's remote workers, permanent, and part-time employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to the company's electronic systems, information, software, and/or hardware.

Confidential Data

Appleton Parish Council defines "confidential data" as:

- Unreleased and classified financial information.
- Customer, supplier, and shareholder information.
- Customer leads and sales-related data.
- Patents, business processes, and/or new technologies.
- Employees' passwords, assignments, and personal information.
- Company contracts and legal records.

Device Security

Company Use

To ensure the security of all company-issued devices and information, Appleton Parish Council employees are required to:

- Keep all company-issued devices, including tablets, computers, and mobile devices, password-protected (minimum of 8 characters).
- Secure all relevant devices before leaving their desk.
- Obtain authorisation from the clerk or assistant clerk before removing devices from company premises.
- Refrain from sharing private passwords with colleagues, personal acquaintances, senior personnel, and councillors.
- Regularly update devices with the latest security software.

Personal Use

Appleton Parish Council recognises that employees may be required to use personal devices to access company systems. In these cases, employees must report this information to management for record-keeping purposes. To ensure company systems are protected, all employees are required to:

- Keep all devices password-protected (minimum of 8 characters).
- Ensure all personal devices used to access company-related systems are password protected.
- Install full-featured antivirus software.
- Regularly upgrade antivirus software.
- Lock all devices if left unattended.
- Ensure all devices are protected at all times.
- Always use secure and private networks.

Email Security

Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs. Therefore, Appleton Parish Council requires all employees to:

- Verify the legitimacy of each email, including the email address and sender name.
- Avoid opening suspicious emails, attachments, and clicking on links.
- Look for any significant grammatical errors.
- Avoid clickbait titles and links.
- Contact the IT department regarding any suspicious emails.

Transferring Data

Appleton Parish Council recognises the security risks of transferring confidential data internally and/or externally. To minimise the chances of data theft, we instruct all employees to:

- Refrain from transferring classified information to employees and outside parties.
- Only transfer confidential data over Appleton Parish Council networks.
- Obtain the necessary authorisation from senior management.
- Verify the recipient of the information and ensure they have the appropriate security measures in place.
- Immediately alert the Parish Council of any breaches, malicious software, and/or scams.