DISLEY PARISH COUNCIL

Cyber Security Policy

Version	Date	Reviewed by:
Original Version	**14/01/2021**	**Disley Parish Council**
V2	**13/01/2022**	**Disley Parish Council**

Introduction
The risk of data theft, scams, and security breaches can have a detrimental impact on the Council's systems, technology infrastructure and reputation. As a result, Disley 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:

1. Protect Disley 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
4. List the company's disciplinary process for policy violations.

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

Confidential Data
Disley Parish Council defines "confidential data" as:

1. Unreleased and classified financial information.
2. Customer and supplier information.
3. Employees' passwords and personal information.
4. Council contracts and legal records.

Device Security

1. **Council Use**

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

1.1 Keep all council-issued devices, including tablets, computers, and mobile devices, password-protected (minimum of 8 characters).
1.2 Secure all devices before leaving their desk.
1.3 Obtain authorisation from the clerk before removing devices from council premises.
1.4 Refrain from sharing private passwords with colleagues, personal acquaintances and councillors.
1.5 Regularly update devices with the latest security software.

2. Personal Use

Disley Parish Council recognises that employees may be required to use personal devices e.g. mobile phones, 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:

2.1 Keep all devices password-protected (minimum of 8 characters).
2.2 Ensure all personal devices used to access council-related systems are password protected.
2.3 Install antivirus software.
2.4 Regularly upgrade antivirus software.
2.5 Lock all devices if left unattended.
2.6 Ensure all devices are always protected.
2.7 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, Disley Parish Council requires all employees to:

1. Verify the legitimacy of each email, including the email address and sender name.
2. Avoid opening suspicious emails, attachments, and clicking on links.
3. Look for any significant grammatical errors.
4. Avoid clickbait titles and links.
5. Contact the Clerk regarding any suspicious emails.

Transferring Data

Disley 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:

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