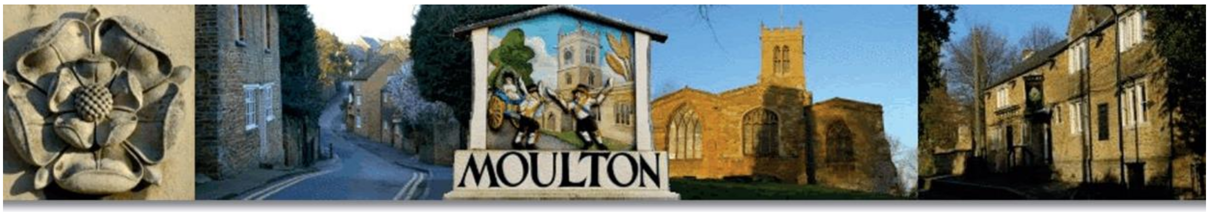

LOCAL COUNCIL
AWARD SCHEME
QUALITY GOLD

Jane Austin
*Executive Officer*

Moulton Parish Council
Moulton Community Centre - Sandy Hill
Reedings, Moulton, Northants, NN3 7AX
**t: 01604 642202**
**e:** info@moultonparishcouncil.org.uk
**w:** www.moultonnorthants-pc.gov.uk

# Information Security Policy (including card payments)

## 1. Purpose and Scope

This document encompasses all aspects of security surrounding confidential information and card payment data and must be distributed to all employees. All employees must read this document in its entirety and confirm they have read and understand this policy fully.

This Policy should be read in conjunction with the Data Protection Policy, Data Breach Policy, General Privacy Notice, General Privacy Notice for Staff, Records Retention Policy, Social Media, Digital and Electronic Communications Policy, and Working from Home Policy.

Ashby Computer Services supply our IT equipment, process our data and manages the following on our behalf:

- Gold Server Software Support
- Ashby Managed Hardware support for Firewall device
- Ashby Managed Hardware support for Switch
- Ashby Managed Hardware support for Wireless Access Point (WAP)

## 2. Legal Responsibility & Policy Support

Data Protection Act 2018
General Data Protection Regulation (GDPR)
Local Government Bodies Regulations 2014

## 3. Cybersecurity

Data security is an ever-increasing risk for most organisations including councils. However, the number of breaches which are the result of highly sophisticated attacks from hackers is still very limited; most breaches are still the result of human error or relatively unsophisticated phishing attacks.

## 4. Card Payments

Moulton Parish Council handles sensitive cardholder information daily via the Square system. Sensitive information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

Moulton Parish Council commits to respecting the privacy of all its customers and to protecting any cardholder data from outside parties. To this end, council is committed to maintaining a secure environment in which to process cardholder information to meet these promises.

Employees handling Sensitive cardholder data should ensure:

- Handle cardholder information in a manner that fits with their sensitivity.
- Do not disclose personnel information unless authorised.
- Protect sensitive cardholder information.
- Keep passwords and accounts secure.
- Request approval from council prior to establishing any new cardholder software or hardware, third party connections, etc.
- Always leave desks clear of sensitive cardholder data and lock away any files or equipment containing such information, when unattended.
- Information security incidents must be reported, without delay, to the Executive Officer and such incidents will be swiftly dealt with and reported.
- We each have a responsibility for ensuring council's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager. Moulton Parish Council will not receive or retain any card details on any form of computer.
- Moulton Parish Council will not receive or retain any cardholder information in any electronic or computer format including emails.
- Cardholder information will only be held in paper format and card details will be protected and all files will be locked away when not in use.

### Suspicious E-mails

Report misleading websites, emails, phone numbers, phone calls or text messages you think may be suspicious.
Do not give out private information (such as bank details or passwords), reply to text messages, download attachments or click on any links in emails if you're not sure they're genuine.
Contact Ashby Computers and forward suspicious emails to report@phishing.gov.uk .

### Public Wi-Fi

Using Public Wi-Fi networks increases the risk of personal information being stolen. Avoid using Public Wi-Fi to access websites containing personal information i.e. emails, banking etc.

## 5. Acceptable use

Employees should:

- be responsible for their own actions and act responsibly and professionally.
- take all necessary steps to prevent unauthorised access to confidential data which includes card holder data.
- keep access to the cardholder equipment secure and do not share passwords or access cards etc.
- authorised users are responsible for the security of these items so they cannot be tampered, altered, or accessed for personal use.
- immediately report any breach to the Executive Officer.
- understand that both business and personal use of our systems can be monitored as appropriate.
- understand that they can use whistleblowing policy if it is believed that someone is misusing Moulton Parish Councils assets, information, or electronic equipment.

Moulton Parish Council will not receive or retain any cardholder information in any electronic or computer format including emails.

## 6. Network Security

Our Network Security is managed by Ashby Computer Services.

## 7. System and Password Security.

Our System and Password Security is managed by Ashby Computer Services

### User IDs and Passwords

Users must:

- Protect usernames and passwords appropriately.
- Create secure passwords.
- Lock the screen when temporarily leaving devices that are in use.
- Log out of all computer devices during non-working hours, i.e., at the end of the working day.

Users must not:

- write down passwords or store in shared folders.
- log on to any DWP systems using another user’s credentials.

## 8. Anti-Virus Software

Our Anti-Virus Software is managed by Ashby Computer Services

## 9. Hardware, Data Encryption and Technology

Ashby Computer Services manage the following on our behalf:

- Laptops & PC’s
- Encrypted backups
- Updates to your computer hardware and software
- Penetration tests with appropriate analysis of results
- Patch Management
- Vulnerability Management
- Configuration Standards
- Audit and Log review

## 10. Remote Access

Moulton Parish Council accesses our server remotely via Ashby Computers VPN.

## 11. Protect Stored Data

All sensitive cardholder data stored and handled by Moulton Parish Council and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by Moulton Parish Council for business reasons must be discarded in a secure and irrecoverable manner.

## 12. Information Classification

It is strictly prohibited to store:

- The contents of the payment card magnetic stripe (track data) on any media whatsoever.

- The CVV/CVC (the 3- or 4-digit number on the signature panel on the reverse of the payment card) on any media whatsoever.

- The Personal Identification Number (PIN) or the encrypted PIN Block under any circumstance

**Card data** and media containing such data must always be labelled to indicate sensitivity level:

**Confidential data** might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to Moulton Parish Council if disclosed or modified. Confidential data includes cardholder data.

**Internal Use data** might include information that the data owner feels should be protected to prevent unauthorised disclosure;

**Public data** is information that may be freely disseminated.

## 13. Access Sensitive Cardholder Data

All Access to sensitive cardholder information should be controlled and authorised. Any job functions that require access to cardholder data should be clearly defined.
Any display of the card number should be restricted at a minimum of the first 6 and the last 4 digits of the cardholder data.
Access to sensitive cardholder information, personal information and business data is restricted to authorised employees that have a legitimate need to view such information.
No other employees should have access to this confidential data unless they have a genuine business need and have authorisation from the Executive Officer.
Any cardholder data should not be shared with a Service Provider (3rd party).

## 14. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.
Media in any digital or physical medium (e.g. printed or handwritten paper, received faxes, USBs, back-up tapes, computer hard drive, etc).
Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.

## 15. Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.
Card holder data must never be sent over the internet via email, instant chat, or any other end user technologies.
If there is a business justification to send cardholder data via email, then it should be done after authorisation and by using a strong encryption mechanism.
The transportation of media containing sensitive cardholder data to another location must be authorised by Executive Offer and must be logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

## 16. Disposal of Data

All data must be disposed of when no longer required by Moulton Parish Council, by the method outlined in our Data Retention Policy.

## 17. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance.

## 18. Security Awareness, Additional Policies and Procedures

The policies and procedures outlined below must be incorporated into council’s practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees.

Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day-to-day practice.
It is required that all employees with contact to card details, confirm that they understand the content of this Information Security policy and read the associated policies where applicable.

- Data Protection Policy
- Data Breach Policy
- General Privacy Notice
- General Privacy Notice for Staff
- Records Retention Policy
- Social Media, Internet Use and Electronic Communications
- Working from Home Policy

**This policy is reviewed annually by the Executive Officer and submitted to the full council for approval.**

| | |
|---|---|
| **Last Reviewed:** | **January 2024** |
| **Review Due:** | **January 2025** |