GDPR DATA PROTECTION POLICY

WARE TOWN COUNCIL

What's in the Policy:

Details on how employees handle sensitive cardholder information. How data is protected in transit and how stored data is disposed of.

Adopted

19th October 2015

For more information please contact:

info@waretowncouncil.gov.uk

Telephone: 01920 460316

Review

September 2020

GDPR DATA PROTECTION POLICY

WARE TOWN COUNCIL

WARE TOWN COUNCIL (the "Council")

PCI INFORMATION SECURITY POLICY

Introduction

This Policy document encompasses all aspects of security surrounding confidential Council information and must be distributed to all Council employees. All Council employees must read this document in its entirety and sign the form confirming they have read and fully understand this policy. This document will be reviewed and updated by the Council on an annual basis or when relevant to include newly developed security standards into the policy and re-distributed to all employees and contractors where applicable.

Information Security Policy

The Council handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect the cardholder data, cardholder privacy, and to ensure compliance with various regulations, along with guarding the future of the organisation.

The Council commits to respecting the privacy of all its customers and to protecting any customer data from outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Employees handling sensitive cardholder data should ensure:

- They handle Company and cardholder information in a manner that fits with their sensitivity and classification;
- They limit personal use of the Council's information and telecommunication systems and ensure it doesn't interfere with their job performance;

- The Council reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- They do not use e-mail, internet and other Council resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- They do not disclose personnel information unless authorised;
- Protection of sensitive cardholder information;
- Keeping passwords and accounts secure;
- They request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- They do not install unauthorised software or hardware, including modems and wireless access unless they have explicit management approval;
- desks are always left clear of sensitive cardholder data and computer screens locked when unattended;
- Information security incidents are reported, without delay, to the Town Clerk or Finance & Admin Manager.
- All POS and PIN entry devices are appropriately protected and secured so they cannot be tampered with or altered.
- They are aware that information contained on any portable computer is especially vulnerable and special care should be exercised.
- That all sensitive cardholder data that is stored and handled by the Council and its employees is securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by the Council for business reasons must be discarded in a secure and irrecoverable manner.

It is strictly prohibited to store:

1. **The contents of the payment card magnetic stripe (track data) on any media whatsoever.**
2. **The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.**
3. **The PIN or the encrypted PIN Block under any circumstance.**

We each have a responsibility for ensuring the Council's systems and data are protected from unauthorised access and improper use. If anyone is unclear about any of the policies detailed herein they should seek advice and guidance from their line manager.

Protecting Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data, etc.) 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 or by any other mode then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, SSL, TLS, IPSEC, etc.).
- The transportation of media containing sensitive cardholder data to another location must be authorised by management, 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.

Disposal of Stored Data

- All data must be securely disposed of when no longer required by the Council, regardless of the media or application type on which it is stored.
- All hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons.
- All hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.

Agreement to Comply Form – Agreement to Comply With Information Security Policies

_____

Employee Name (printed)

_____

Department

I agree to take all reasonable precautions to assure that Council internal information, or information that has been entrusted to the Council by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with the Council, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the Town Clerk.

I have access to a copy of the PCI Information Security Policy, I have read and understand this policy, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the Town Clerk or Finance & Admin Manager.

_____

Employee Signature

_____

Date