GDPR CMPC Information Security Policy Addendum Part 1&2

Combe Martin Parish Council 23-05-2018 (CMPC)

1. Credit or Debit card Payments

Customer credit or debit cards are accepted at the Parish Council Desk only.
No card details are registered, the merchant's copy of the payment receipt is kept in a separate file.
All transactions are processed through Worldpay.
Card Processing is through the hand-held device provided by Worldpay who also process each transaction via a telephone line.
Transaction details are accessed through the secure login Worldpay website for Parish Council accounts purposes only.

Information Security Policy – Employee/Councillor Commitment

Authorised CMPC employees handle sensitive cardholder information daily and each employee commits to respecting the privacy of all its customers and to protecting any customer data from outside parties.

Employees handling cardholder data should:

- Ensure all cardholder information is handled in line with the Worldpay agreement;
- Limit personal use of the Council's information and telecommunication systems to ensure it doesn't compromise security;
- Not use e-mail, internet and other CMPC resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Not disclose personnel information unless authorised;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure;
- Be cautious when opening e-mail attachments received from unknown senders, these may contain viruses, e-mail bombs, or Trojan horse code;
- Request approval from the Clerk prior to establishing any new software or hardware, third party connections, etc.;
- Not install unauthorised software or hardware, including modems and wireless access unless you have explicit approval;
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
- Report information security/data incidents to the Clerk and inform the Data Protection Officer.

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.

- A list of devices that accept payment card data should be maintained.
- The list should include make, model and location of the device.
- The list should have the serial number or a unique identifier of the device.
- The list should be updated when devices are added, removed or relocated.

Disposal of Stored Data

- All data must be securely disposed of when no longer required by CMPC, regardless of the media or application type on which it is stored.
- All hard copies of personal data must be manually destroyed when no longer required for valid and justified business reasons.
- CMPC will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- CMPC will have documented procedures for the destruction of electronic media.

Breach Response

If CMPC reasonably believes it may have an account breach, or a breach of cardholder information, the Clerk must inform Worldpay.
CMPC employee to immediately inform the Clerk and Worldpay.
CMPC Clerk/employee to inform the CMPC Chair and Data Protection Officer.
Once the initial facts and the extent of the breach have been established, the Clerk is to inform the Information Commissioner's Office.

2. Car Park Permits

Car Park Permits require the permit Holder to provide contact and vehicle details which are entered onto a spreadsheet for council office use only.
Holder and vehicle details are kept on a spreadsheet accessed by Parish council staff only through password protected computer logins.
This information is held on the Parish Council Server based at the Seacott Office address.

(NB. Car park and dog fouling enforcement - Section under preparation and to follow).

Employee/Councillor Commitment

We each have a responsibility for ensuring our CMPC 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 the Clerk.
The CMPC has a Data Protection and Information Security Policy, Website Compliance Notice and Impact Assessment Document.
This when linked with the need for verbal confidentiality, encompasses all aspects of security surrounding confidential council information.
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;

All employees/councillors need to be informed of the legal obligations and must read these documents and sign confirming they have read and fully understand the policies. This document will be reviewed and updated by the Data Protection Officer/Clerk as required or on an annual basis.

_____
Name (printed)

_____
Role

I have read and understood the CMPC Policies and Guidance on the General Data Protection Regulation (GDPR)

_____
Signature

Date:

Version: 1