COMPTON PARISH COUNCIL

Data Protection Policy

May 2018

Context and Overview

- Policy prepared by: The Clerk, Mrs Joanna Cadman
- Approved by Parish Council on: 16th May 2018
- Policy became operational on: 17th May 2018
- Next review date: Annual Meeting, 2019

INTRODUCTION

Compton Parish Council needs to gather and use certain information about individuals. These can include parishioners, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Parish Council's data protection standards – and to comply with the law.

WHY THIS POLICY EXISTS

This data protection policy ensures that Compton Parish Council

- Complies with data protection law and follows good practice
- Protects the rights of staff, parishioners and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

DATA PROTECTION LAW

The Data Protection Act 1998 describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA) unless that country or territory also ensures an adequate level of protection

People, Risks and Responsibilities

POLICY SCOPE

This policy applies to:

- Compton Parish Council
- All staff, councillors and volunteers of Compton Parish Council
- All contractors, suppliers and other people working on behalf of Compton Parish Council

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

DATA PROTECTION RISKS

This policy helps to protect Compton Parish Council from some very real data security risks, including:

- **Breaches of confidentiality:** for instance, information being given out inappropriately.
- **Failing to offer choice:** for instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage:** for instance, the company could suffer if hackers successfully gained access to sensitive data

RESPONSIBILITIES

Everyone who works with or for Compton Parish Council has some responsibility for ensuring data is collected, stored and handled appropriately.

- **Councillors** are ultimately responsible for ensuring that Compton Parish Council meets its legal obligations

- **The Data Protection Officer** (to be appointed) is responsible for:
  i. Keeping councillors updated about data protection responsibilities, risks and issues
  ii. Reviewing all data protection procedures and related policies, in line with an agreed schedule
  iii. Arranging data protection training and advice for the people covered by this policy
  iv. Handling data protection questions from anyone covered by this policy
  v. Dealing with requests from individuals to see the data Compton Parish Council holds about them (also called subject access requests).
  vi. Checking and approving any contracts or agreements with third parties that may handle the Parish Council's sensitive data.

- **The Clerk** is responsible for:
  i. Ensuring all systems, services and equipment used for storing data meet acceptable security standards

ii. Performing regular checks and scans to ensure security hardware and software is functioning properly
iii. Evaluating any third party services the Parish Council is considering using to store or process data. For instance, cloud computing services.

General Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally.
- Compton Parish Council will ensure that its employees have access to training to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guideline below.
- In particular, strong passwords should be used and they should never be shared.
- Personal data should not be disclosed to unauthorized people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Data Storage

These rules describe how and where data should be safety stored.

Paper Storage

When data is stored on paper it should be kept in a secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.

- When not required, the paper or files should be kept in a locked drawer or filing cabinet
- Employees should ensure paper and printouts are not left where unauthorized people could see them, eg: on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

Electronic Storage

When data is stored electronically it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared.
- If data is stored on removable media these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location.
- Data should be backed up frequently. These backups should be tested regularly.
- Data should never be saved directly to laptops or other mobile devices such as tablets or smart phones.

- All servers and computers containing data should be protected by approved security software and a firewall

Data Use

- When working with personal data, employees should ensure that the screens of their computers are locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email.
- Data must be encrypted before being transferred electronically.
- Personal data should never be transferred outside the European Economic Area
- Personal data should not be stored on personal computers.

Data Accuracy

The law requires Compton Parish Council to take reasonable steps to ensure data is kept accurate and up to date.

- Data will be kept in as few places as necessary.
- Every opportunity should be taken to ensure data is updated.
- Compton Parish Council will make it easy for data subjects to update the information is holds on them, eg: via the Parish Council website.
- Data should be updated as inaccuracies are discovered.

Subject Access Requests

All individuals who are the subject of personal data held by Compton Parish Council are entitled to:

- Ask what information the Parish Council holds about them and why.
- Ask how to gain access to it.
- Be informed about how to keep it up to date.
- Be informed how the company is meeting its data protection obligations

A request from an individual for this information is a Subject Access Request.

Subject access requests should be made by email, addressed to the data controller.

Individuals will not be charged unless the request is considered repetitive or vexacious, when they will be charged £10 per subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before giving information.

Disclosing data for other reasons

In certain circumstances the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Compton Parish Council will disclose the requested data. The data controller will ensure the request is legitimate.

Providing information

Compton parish Council aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, Compton Parish Council has a privacy statement setting out how data relating to individuals is used by the authority.

This is available on request and is also available on the Parish Council's website.