# Brewood and Coven Parish Council

## Information Security Policy

**(For internal use only – to be distributed to all employees and Parish Councillors)**

### Opening statement

Brewood and Coven Parish Council is committed to preserving the confidentiality, integrity and availability of the personal data of the individuals (employees and others) it deals with.

Personal data is defined as **any** information that relates to an identified or identifiable person. It can be held in either electronic or hard copy form.

The Parish Council recognises that some personal data is legally regarded as 'special' such as information about a person's health, ethnicity, etc. and that this warrants greater care in its handling. Other information whilst not strictly 'special' such as disciplinary records, payroll information etc. should be treated with an equal level of care.

Unauthorised access to information or loss/ destruction can lead to complaints, civil claims, fines from the Information Commissioner and reputational damage.

It is recognised that breaches of information security can be caused internally or externally, deliberately or accidentally.

### Assets

The Parish Council has conducted a data audit/flow exercise to record what personal data it processes, why, how and the way it flows in to, through and outside of the Parish Council. It is also aware of what physical assets are used for the processing of information.

The purpose of this exercise was so as to inform the Parish Council of the potential threats to information/physical assets, the likelihood of any threat occurring and the impact if a threat were to occur.

The person responsible [the 'asset owner'] for the information and physical assets is the Clerk – Maggie Birtles.

### Objective of this policy and associated procedures

The Parish Council seeks to reduce the risk of a breach of its security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal information transmitted, stored or otherwise processed.

Examples of a breach of security would be:
a) an employee securing access to the personal information of another individual that they have no justifiable need to see;
b) the sending of information by email to the wrong recipient.
c) leaving paper based information on a bus or a train.

### Methodology

The Parish Council intends to ensure the **confidentiality, integrity and availability** of information by taking general measures as identified below and the issue and adoption of the attached guidelines/

procedures. The Parish Council believes that this course of action will reduce the identified risk to a level acceptable to the Parish Council.

The specific guidelines/procedures will cover such subjects as:

a) the acceptable use of information and physical assets
b) physical security
c) disposal of records/ hardware
d) transmission of information
e) relationships with data processors.

The Parish Council will also ensure that it has the ability to **restore** the availability of and access to information in a timely manner in the event of a security incident or other event.

**General measures**

**Internal threats**

To deal with any internal threat the Parish Council will, where appropriate and lawful, carry out pre-employment screening checks of all potential employees who will have access to information as part of their duties.

Contracts with those employees will stress the importance of compliance with this policy and any supporting procedures and the consequences of failure to comply.

The Parish Council will ensure that employees who have access to/ use of information only have access to that which they need to in order to fulfil their role. Any employee who leaves the employment of the Parish Council will have their rights of access to information revoked on the day of departure.

Any physical Parish Council assets in the possession of an employee **must** be returned to the Parish Council by departure day at the latest.

**Training/awareness**

The Parish Council recognises that threats to information are continually evolving. As such the Parish Council will provide those employees who handle personal information with awareness training as and when appropriate.

**Malware**

The Parish Council will put in place measures to prevent and detect malware and thus to protect information. The Parish Council will also have in place measures that enable recovery of information in the unlikely event that information is compromised. The primary measure will be by ensuring that all information is backed up/ copied and placed/ stored in a secure off- site location.

**Procedure in the event of a security incident.**

In the unlikely event that there is a breach of our security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to information then employees or parish councillors should inform the Clerk **immediately** upon discovery. The Clerk will ensure that the following steps are taken:

**Contain and recover**

Having ensured that there are appropriate resources available it will be established who needs to be made aware of the breach and inform them of what they are expected to do to assist in any containment exercise. It will also established whether anything can be done to recover any losses and limit the damage the breach can cause. In appropriate cases the *Police* may be informed.

There should be an assessment of the potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen. There will need to be a consideration of the following:

a) What type of data is involved?
b) How sensitive is it?
c) If data has been lost or stolen, are there any protections in place such as encryption?
d) What has happened to the data?
e) Regardless of what has happened to the data, what could the data tell a third party about the individual?
f) How many people are affected by the breach?
g) Who are the people whose data has been breached?
h) What harm can come to the individual(s)?
i) If individual bank details have been lost, we should consider contacting the banks themselves for advice on anything they can do to help prevent fraudulent use.

**Notification of breaches**

The Parish Council will (unless it is **unlikely** that there is a risk to the individual concerned) notify the Information Commissioner's Office. It will do so without undue delay and where feasible not later than 72 hours after first becoming aware of the breach.

The Parish Council will (when dealing with the Commissioner's office):

(a) *describe* the nature of the breach including where possible, the categories and approximate number of people affected and the categories and approximate number of personal data records concerned;
(b) *communicate* the name and contact details of the Data Protection Officer where more information can be obtained;
(c) *describe* the likely consequences of the personal data breach;
(d) *describe* the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
If the breach is likely to result in a **high risk** to the individuals interests the Parish Council will communicate the fact of the breach to them without undue delay.
It will:

(a) *communicate* the name and contact details of the Data Protection Officer -where more information can be obtained;
(b) *describe* the likely consequences of the breach; and
(c) *describe* the measures taken or proposed to be taken by us to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

**Evaluation and response**

After the breach the Parish Council will establish the cause of the breach and evaluate the effectiveness of its response. If the breach was caused, even in part, by systemic and ongoing problems, then simply

containing the breach and continuing with 'business as usual' is not acceptable; similarly, if the Parish Council's response was hampered by inadequate policies or a lack of a clear allocation of responsibility then there will be a review and update of these policies and lines of responsibility- in the light of the breach experience.

**Conclusion**

This policy and associated procedures will be reviewed and amended periodically or, as outlined above, in the event of a security incident or other event.

The policy and procedures have been approved by the Parish Council.

Employees and Parish Councillors are obliged to comply with this policy and procedures when processing information on our behalf.

All employees and Parish Councillors who process personal data are required to read the policy/ procedures and indicate that they understand it. If anybody requires clarification of the policy/ procedures/ guidelines they should speak with Maggie Birtles.

Version 2

Approved by Parish Council (to take effect on 25 May 2018) 12th April 2018

Persons responsible for compliance – all Parish Councillors

Review date 13 June 2019