Brewood and Coven Parish Council

Data Protection Policy

Opening Statement

Brewood and Coven Parish Council (collectively all of our Parish Councillors) is committed to complying with both the General Data Protection Regulation ('GDPR') and the Data Protection Act 2018. This policy sets out how we handle the personal data of our employees and other individuals.

The law applies to any information we control that relates to an identified individual or someone who can be identified from the information.

This policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, volunteers or other individuals.

The law applies to information processed by automated means such as computers, phones, or held in a relevant filing system for example an employee's personal file- or it is information intended to form part of such a file.

As a public authority we recognise that the correct and lawful treatment of this information will maintain the confidence of our employees and others in us. Protecting the confidentiality and integrity of personal data is something that the Parish Council takes extremely seriously. The Parish Council is exposed to potential fines of up to EUR20 million depending on the breach, for failure to comply with the provisions of the GDPR.

This policy applies to all employees and Parish Councillors. Employees and Parish Councillors **must** read, understand and comply with this policy when processing personal data on our behalf. This policy sets out what the Council expects from employees and Parish Councillors in order for the Council to comply with the law. Compliance with this policy is mandatory. Related policies and procedures/ guidelines are available to help you interpret and act in accordance with this policy. You must also comply with the related documents. Any breach of this policy may result in disciplinary action.

This policy and the related documents are for internal use only and cannot be shared with third parties without prior authorisation of the Council.

The Parish Council is ultimately responsible for securing compliance with this policy. Day to day enquiries should however be passed to the Clerk –Maggie Birtles.

~~**Data Protection Officer**~~

~~The Council's formally appointed Data Protection Officer is Mr David Campbell. They can be contacted via the Parish Council. Their role, amongst other matters, is to:~~
~~a) inform and advise the Council of its obligations under GDPR and other UK or European data protection law;~~
~~(b) to monitor the Council's compliance with the law and with our internal data protection policies/ procedures;~~
~~(c) to provide advice where requested as regards any data protection impact assessment and to monitor its performance;~~
~~(d) to co-operate with the Information Commissioner.~~

~~The Council will ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. The Council will support the data protection officer~~

~~in performing their tasks by providing resources necessary to carry out those tasks and by allowing access to personal data and our processing operations.~~

~~The Council will ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. The Council will not seek to dismiss or penalise them as a result of them performing their tasks. The data protection officer must be allowed to directly report to full Council as and when appropriate.~~

Definitions of terms used in this document and examples

We process **personal data**. As regards employees this is detailed on our data audit document but typically comprises information held on offers of employment, employee reviews, financial information etc. We process the personal data of volunteers and applicants for grants and other individuals who have a connection to the Council.

Special personal data is that about an individual's race/ethnicity, political opinions, religious or philosophical beliefs, their genetic, biometric or health information or their sex life or sexual orientation.

Processing includes receiving information, storing it, considering it, sharing it, destroying it etc. We recognise that the law applies to all processing activities whether we control information or we process upon the instructions of an insurer client.

A **processor** is a non-employee organisation/third party who process employee information, on our behalf and to our instructions.

We are the **controller** as regards personal data as we determine what is collected, why and how it is used within our business. We are registered with the Information Commissioner under reference **xxx**

The employee or other individual is the **subject** of the information.

A **data breach** means a breach of our security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

This policy should be read alongside the Council's information security policy.

Commitment to the (General Data Protection) principles

The Council (through its employees and Parish Councillors) will:

(a) process personal data **fairly, transparently** and only if there is a **legal basis** to do so.

As part of this we will inform individuals (concisely and using clear and plain language so that they understand) of the following:

1) that we are the 'data controller';
2) our contact details;
3) the name and contact details for the data protection officer;
4) the purposes for the processing of their information and the legal basis for the same;
5) the identity of any person/organisation to whom personal data may be disclosed;
6) whether we intend to process personal data outside the European Economic Area;
7) how long (as best we can) we will hold their information;
8) their rights.

(b) only collect personal data for **specified, explicit and legitimate** purposes. We must not further process any information in a manner that is **incompatible** with those original purposes;

(c) ensure that the personal data we collect is **adequate, relevant and limited** to what is **necessary** to carry out our functions etc. We must only collect the personal data that is required to undertake our duties: we must not collect excessive data. We must ensure that any personal data collected is adequate and relevant for the intended purposes. We must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised;

(d) ensure that the personal data we process is **accurate** and, where necessary, **kept up to date**. We must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

(e) keep personal data in a form that identifies employees or other individuals for **no longer than is necessary** for the purposes that it was obtained.

The Council will periodically review what personal data is held and erase/destroy that which is no longer needed.

(f) process personal data (whatever the source) in a manner that ensures **appropriate** security of the same including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Employees and Parish Councillors are responsible for protecting the personal data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against any accidental loss of, or damage to it. Employees and Parish Councillors must exercise particular care in protecting special personal data from loss and unauthorised access, use or disclosure.

Employees and Parish Councillors must follow all procedures and technologies the Council puts into place to maintain the security of personal data from the point of collection to the point of destruction. Employees and Parish Councillors must maintain data security by protecting the confidentiality, integrity and availability of personal data. This is defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.
(b) Integrity means that personal data is accurate and suitable for the purpose for which it is processed.
(c) Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

This is elaborated upon in our information security policy.

Employees and Parish Councillors must comply with all applicable aspects of our information security policy and not attempt to circumvent the administrative, physical and technical safeguards we have in place.

The Council is responsible for, and must be able to demonstrate, compliance with the six principles detailed above.

Personal data breaches

The Council will usually be required to notify any personal data breach to the Information Commissioner and, in certain instances, the affected individual as well.

We have put in place procedures to deal with any suspected personal data breach and will notify individuals and the Information Commissioner where we are legally required to do so.

If employees or Parish Councillors know or suspect that a personal data breach has occurred they should contact the Data Protection Officer **immediately**. Any evidence relating to the potential breach should be preserved.

Legal basis for processing employee and other individual personal data

The Council generally processes **employee** personal data in the following circumstances:

(a) To *perform a contract* where the employee is a party or *in order to take steps* at the request of the employee prior to entering into a contract;
(b) Where processing is *necessary for compliance with our legal obligations,* for instance, health and safety, payroll;
(c) to further our *legitimate interests.*

We process **individual** client personal data so as to:

(a) perform a contract for the provision of services by us or to take steps at their request prior to entering into a contract;
(b) with their consent;
(c) in the public interest or in the exercise of official authority by us

**Employees and Parish Councillors must always ensure that they have a lawful basis to process personal data before they process it. **

Consent

If the Council processes personal data with a person's consent then for it to be valid consent the individual concerned **must** indicate agreement clearly either by a statement or positive action. Consent requires affirmative action so silence or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Individuals must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if the Council intends to process personal data for a different and incompatible purpose which was not disclosed when the individual first consented.

The Council will need to prove that consent was given. Employees must keep records so that we can demonstrate compliance with the law.

Special (sensitive) personal data

The Council will **only** process this kind of information where an exception applies i.e. where it is necessary for employment/social security purposes or, again, necessary for the purposes of preventative or occupational medicine [delegated to a health care professional] so as to assess the capacity of the employee to work.

If the Council relies on consent then this must be **explicit** i.e. employees must set out in writing what it is that the Council wishes to do with the information and the individual must sign to indicate acceptance. As above a record must be kept.

DBS/ criminal record checks

The Council may arrange for these to be undertaken. Results of a DBS check are processed only until the Council is satisfied that a volunteer has an acceptable record. The DBS check is then destroyed/ erased. However the fact that a volunteer has an acceptable record is noted so that proof can be supplied to persons with a justifiable interest in knowing.

Rights

Individuals have rights when it comes to how we handle their personal data. These include rights to:
(a) withdraw consent to processing at any time;
(b) receive certain information about our processing activities;
(c) request access to their personal data that we hold;
(d) prevent our use of their personal data for direct marketing purposes;
(e) ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
(f) restrict processing in specific circumstances;
(g) challenge processing which has been justified on the basis of our legitimate interests;
(j) prevent processing that is likely to cause damage or distress to them or anyone else;
(k) be notified of a personal data breach which is likely to result in high risk to their rights and freedoms, and,
(l) make a complaint to the Information Commissioner.

Employees **must** verify the identity of an individual requesting data under any of the rights listed above. Employees must not allow third parties to persuade them into disclosing personal data without proper authorisation.

You must immediately forward any request you receive to the Clerk.

In certain circumstances we are permitted to restrict the above rights. Any restriction will be in accordance with the law.

Council use of processors

When using processors (people who process employee and other individual personal information on our behalf to our order) the Council will ensure that:

a) it only uses processors who provide sufficient guarantees of having implemented appropriate technical and organisational measures to satisfy us that personal data will be safe.
b) that the chosen processor does not engage another processor without our written authorisation.
c) that any processing is governed by a contract that is binding on the processor and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing and the type of personal data.
d) that the processor will only process the personal data on documented instructions from us.
e) that any person or organisation authorised to process personal data have committed themselves to confidentiality.
f) that the processor deletes or returns all personal data to us after the end of the provision of the processing services.

g) that the processor makes available to us all information necessary to demonstrate compliance with the above and to allow for and contribute to audits, including inspections etc.

Sharing of personal data

Generally we are not allowed to share a person's personal data with third parties unless certain safeguards and contractual arrangements have been put in place.
Employees and Parish Councillors may only share the personal data we hold with third parties if:
(a) they have a need to know the information for the purposes of providing contracted services;
(b) sharing the personal data complies with the fair processing notice provided to the individual and, if required, their consent has been obtained;
(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

Changes to this policy

The Council reserves the right to change this policy at any time. If it does it will draw any changes to the attention of employees.

Approved by Brewood and Coven Parish Council (to take effect on 25 May 2018)

12th April 2018.

Persons responsible for compliance – all Parish Councillors

Version 1

Review date 1 June 2019

Acknowledgement of receipt and review

I, ……, acknowledge that on 10 May 2018, I received and read a copy of Brewood and Coven Parish Council's data protection policy.

I understand that the information in this policy is intended to help the Parish Council to work effectively and assist in the use and protection of personal data.

Signed …….

Printed Name …….

Date …….