BROMSBERROW PARISH COUNCIL

Data Protection Policy - Adopted 30th March 2021

1. Aims

Our Parish Council aims to ensure that all personal data collected about staff and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: ● Name (including initials) ● Identification number ● Location data ● Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs ● Trade union membership ● Genetics ● Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes ● Health – physical or mental ● Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organization that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

4. Roles and responsibilities

This policy applies to all staff employed by our Parish Council and to external organizations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

4.1 Parish Council

The Parish Council has overall responsibility for ensuring that the Parish Council complies with all relevant data protection obligations.

4.2 Data Protection officer

The Parish Council do not need to appoint a DPO.

4.3 Data Processor – The Clerk

The Clerk acts as the representative of the data controller on a day-to-day basis.

5. Data protection principles

The GDPR is based on data protection principles that our Parish Council must comply with.
The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed and destroyed securely.
- Processed in a way that ensures it is appropriately secure

6. Collecting personal data

6.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Parish Council can fulfil a contract with the individual, or the individual has asked the Parish Council to take specific steps before entering into a contract
- The data needs to be processed so that the Parish Council can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the Parish Council, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the Parish Council or a third party (provided the individual's rights and freedoms are not overridden)
- The individual has freely given clear consent.

7 Limitation, minimization and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and will seek consent where necessary.

We will not normally share personal data with anyone else, but may do so where:

- We need to liaise with other agencies – we will seek consent as necessary before doing this
- We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:
- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymized or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

8. Subject access requests and other rights of individuals

8.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Parish Council holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been or will be shared with
- How long the data will be stored for
- The source of the data, if this was not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the Clerk. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

8.2 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of an individual

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

8.3 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information about how we use and process their data, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

9. Data security and storage of records

We will protect personal data and keep it safe from unauthorized or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use

- Papers containing confidential personal data will not be left visible or used in notice boards, or left anywhere else where there is general access
- Secure passwords are used to access computers, laptops and other electronic devices. Employees and Councilors are reminded to change their passwords at regular intervals
- Protection software is used on all office devices and removable media, such as laptops and USB devices.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

10. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Parish Council's behalf. If we do so, we will require the third party to provide guarantees that it complies with data protection law.

11. Personal data breaches

The Parish Council will take all reasonable steps to ensure that there are no personal data breaches.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches may include, but are not limited to:

- Non-anonymized data being published on the Parish Council website which shows personal data
- The theft of a laptop or device containing non-encrypted personal data about individuals

12. Training

All Employees and Councilors are provided with the data protection policy as part of their induction process.

Data protection will also form part of continuing information flow where changes to legislation or guidance make it necessary.

13. Monitoring arrangements

This policy will be reviewed and updated as and when necessary and changes will be shared with and agreed by the full Parish Council, this policy will be reviewed.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the Clerk will immediately investigate and determine whether a breach has occurred. To decide, the Clerk will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The Clerk will alert the Parish Council.
- The Clerk will make all reasonable efforts to contain and minimise the impact of the breach, assisted by Councillors where necessary.
- The Clerk will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The Clerk will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the Clerk will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the Clerk must notify the ICO.
- The Clerk will document the decision (either way), in case it is challenged later by the ICO or an individual affected by the breach. Documented decisions are stored by the Parish Council and/or the Clerk using an appropriate system.
- Where the ICO must be notified, the Clerk will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the Clerk will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the Clerk
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and to mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the Clerk will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the Clerk expects to have further information. The Clerk will submit the remaining information as soon as possible

- The Clerk will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Clerk will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the Clerk
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The Clerk will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The Clerk will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored using an appropriate system.
- The Clerk and Parish Council will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimize the impact of data breaches

Any data breach requires action to mitigate its impact. As a breach could take many different forms and severities, each will need to be assessed and the appropriate actions decided on a case-by-case basis. The following examples provide generic steps and some specific examples. After any breach, we will review the effectiveness of these actions and amend them as necessary.

Basic principles:

- Any employee or Parish Councilor who becomes aware of a breach must alert the Clerk.
- Assess the type, amount and sensitivity of the data involved in the breach.
- Attempt to recall the data as quickly as possible; this may include recalling emails, removing from website/social media or other internet sites.
- Contact any individual or organization directly and explain that the information was sent in error, and request that they delete the information and do not share, publish, save or replicate it in any way
- The Clerk will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The Clerk will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted