

BOBBINGTON PARISH COUNCIL

SOUTH STAFFORDSHIRE

Data Protection Policy

Opening statement

Bobbington Parish Council ('the council') is committed to complying with both the General Data Protection Regulation ('GDPR') 2016/679 and the Data Protection Act 2018. This policy sets out the council's approach (through its Clerk and members) to the handling of personal data.

As a council we recognise that the correct and lawful treatment of people's personal data will maintain their confidence in us and will provide for successful operations.

Protecting the confidentiality and integrity of personal data is something that the council takes extremely seriously. The council is exposed to potential fines of up to EUR20 million (depending on the nature and severity of the infringement) for failure to comply with the provisions of the GDPR.

Both our Clerk and members **must** comply with this policy when processing personal data on the council's behalf.

Compliance with this policy is **mandatory**.

Any breach of this policy or the related policies and procedures/ guidelines may result in disciplinary action or action under the council's code of conduct

Common terms and application

Personal data - this is any information relating to an identified or identifiable living individual.

This policy applies to all personal data the council processes regardless of the media on which that data is stored.

The law (and this policy) applies to

- 1) personal data processed by automated means such as computers, phones, tablets etc. or,
- 2) (structured) personal data held in a 'relevant filing system' for example an employee's personnel file or it is intended to form part of such a file or,
- 3) it is unstructured personal data.

Special personal data is that about an individual's race/ ethnicity, political opinions, religious or philosophical beliefs, membership of a trade union, their genetic/ biometric data (if used to identify them), health information or information about their sex life or sexual orientation.

Processing includes receiving information, storing it, considering it, sharing it, destroying it etc. The council recognises that the law applies to all processing activities

Data Protection Policy

Adopted: 01/08/2021

Date of last review: 17/07/2024

Date of next review: 15/07/2026

The council is the **controller** of people's personal data as we determine what is collected, why and how it is used.

The individual who is the focus of the information is known as the **data subject**.

Consent means any freely given, specific, informed and unambiguous indication of a person's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

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

Commitment to the (General Data Protection) principles

The council will:

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

To comply with this the Council will inform individuals when collecting their personal data (concisely and using clear and plain language so that they understand) of the following:

- 1) that the council is the "data controller"
- 2) our contact details;
- 3) why we are processing their information and in what way the law allows it;
- 4) if we [this will be rare] rely on our 'legitimate interests' for processing personal data we will tell them what those interests are;
- 5) the identity of any person/ organisation to whom their personal data may be disclosed,
- 6) how long we will store their information, and,
- 7) their rights

[more information is given below]

- (b) only collect personal data for **specified, explicit and legitimate** purposes. The Council will process any personal data in a manner that is **incompatible** with the original purpose(s) the data was to be used for;
- (c) ensure that the personal data we collect is **adequate, relevant and limited** to what is **necessary** to carry out the purpose(s) it was obtained for;
- (d) ensure that the personal data we process is **accurate** and, where necessary, **kept up to date**.
- (e) keep personal data in a form that identifies individuals for **no longer than is necessary** for the purpose(s) that it was obtained.

Data Protection Policy

Adopted: 01/08/2021

Date of last review: 17/07/2024

Date of next review: 15/07/2026

The Council will periodically review what personal data is held and erase / destroy or anonymise 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.

The Council will have regard to what the risks to personal data are e.g. loss, theft, damage etc. It will assess the harm that could result if a risk were to materialise and, having done so, put in place appropriate measures to control the risks i.e. to keep the personal data confidential, intact and available for use. Personal data will only be available to those who need to know/ use the information. Personal data should not be shared outside of the Council unless it is legal/ justifiable to do so.

Hard copy information will be stored in a safe and secure location. Electronic data will be encrypted where appropriate and backed-up.

Action in the event of a Personal Data Breach

If the above should occur i.e. personal information is lost or disclosed to someone with authority then the Council needs to investigate matters.

If there is any risk of harm to an individual as a result of the breach then the Council must inform the Information Commissioner's Office. The Council will advise as to a) what has gone wrong, b) the number of people affected, c) the likely consequences for those people and, d) what the Council is doing to put matters right/ mitigate any harm. We must also provide a contact point at the Council for the ICO.

The above report must be made as soon as possible after discovery of the breach or at the latest within 72 hours.

If there is a high risk of harm to individuals then we must also advise them of a), c) and d) above and provide a contact point.

Accountability

The council is responsible for and must be able to demonstrate that it complies with all the above principles.

Legal basis for processing ordinary personal data (article 6)

The council must generally process personal data **ONLY** if one or more of the following circumstances exist:

- (a) Where an individual has given [valid- see definition] **consent**;

- (b) Where necessary to **perform a contract** to which the individual is a party or **to take steps** at their request prior to entering into a contract;
- (c) Where processing is necessary for the council to comply with our **legal obligations**;
- (d) Where processing is necessary for the performance of **a task carried out in the public interest** by the council or it is in the **exercise of official authority** vested in us;
- (e) to further the council's [this will be rare] **legitimate interests or those of a third party** except where such interests are overridden by the privacy interests of the individual who is the subject of the information especially if they are a child.

The Council will always ensure that it has a lawful basis to process personal data **before** they process it. No single basis is 'better' or more important than the others.

Special personal data (article 9)

The council **MUST** only process this kind of information where circumstances exist such as:

- a) the individual has given **explicit** consent for one or more **specified** purposes;
- b) it is necessary for **employment/ social security/ social protection law** purposes;
- c) it is necessary in relation to **legal claims**, or,
- d) it is necessary for reasons of **substantial public interest**.

Rights

Individuals may have rights when it comes to how the council handles their personal data. These, depending on the nature of processing, may include rights to:

- (a) withdraw consent to processing at any time;
- (b) receive certain information when the council collects their information or receives it from a third party;
- (c) request access to their personal data;
- (d) have the council correct inaccurate information;
- (e) ask the council to erase their personal data;
- (f) restrict the way the council uses their information;
- (g) be notified about any recipients of their personal data when they have asked for rectification, erasure or restriction;
- (j) object to any processing undertaken by the council in the public interest/ exercise of official authority or in our legitimate interests or those of another;

(k) object to direct marketing by the council, and, to

(k) be notified by the Council of a personal data breach where it is likely to result in a “high risk” to their rights and freedoms.

Procedures exist (which should be followed) if a person seeks to exercise some of the above rights.

Restrictions

In certain circumstances we are permitted to restrict the above rights and our obligations as well as depart from the principles. Any restriction will be in accordance with the law.

Records of processing activities

The council is obliged to maintain a record of our processing activities. The record will contain, amongst other matters, information about:

- (a) why we process personal data;
- (b) describe the categories of individuals and the categories of personal data;
- (c) state the categories of recipients to whom personal data has been or will be disclosed to;
- (f) where possible, state the envisaged time limits for erasure of the different categories of data;
- (g) where possible, give a general description of the technical and organisational security measures that the council has in place.

The Council will keep the record under review and update it where necessary

Further information

The collective members of the Parish Council are responsible for ensuring that this policy and the related documents are complied with. However, if you have any questions about the policy or any other data protection documentation please speak with the Chair.

Changes to this policy

The council reserves the right to change this policy at any time.

Approved by Victoria Evans – Clerk to the Council (as advised by SSDC Legal team)

Persons responsible for compliance – all Councillors