Postling Parish Council

Data Protection Policy

Introduction

Postling Parish Council (PPC) collects and uses certain types of personal information about councillors, residents, staff and other individuals who encounter the council and its employees.

PPC may be required by law to collect and use certain types of information to comply with statutory obligations related to employment.

This policy is intended to ensure that personal information is dealt with properly and securely, and in accordance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and other related legislation.

GDPR applies to all computerised data and manual files if they come within the definition of a filing system and includes PPC's website domain and official email address.

Personal Data is defined as information that identifies an individual. A sub-set of personal data is known as 'personal sensitive data'. This special category data is information that relates to a person's:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Physical or mental health
- An individual's sex life or sexual orientation
- Genetic or biometric data for the purpose of uniquely identifying a natural person.

Personal sensitive data is given special protection, and additional safeguards apply if this information is to be collected and used.

PPC does not intend to seek or hold sensitive personal data about staff or clients except where it has been notified of the information, or it comes to light via legitimate means (e.g., a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice.

To mitigate risk, all electronic communications will be conducted through the council's clerk@postling-pc.gov.uk email address. The Data Protection Principles (Article 5 of the GDPR) sets out six data protection principles which must be followed at all times:

1) Personal data shall be processed fairly, lawfully and in a transparent manner.

2) Personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes.

3) Personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed.

4) Personal data should be accurate and, where necessary, kept up to date.

5) Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes.

6) Personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures. In addition to this, PPC is committed to always ensuring that, anyone dealing with personal data shall be mindful of the individual's rights under the law.

PPC is committed to always complying with the Data Protection Principles. This means that we will:

- Inform individuals as to the purpose of collecting any information from them, as and when requested.
- Identify who we will share the information with and how long PPC will retain this information.
- Be responsible for checking the quality and accuracy of the information.
- Regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy.
- Ensure that when information is authorised for disposal it is done in accordance with our disposals policy.
- Ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system and always follow the relevant security policy requirements.
- Share personal information with others only when it is necessary and legally appropriate to do so.
- Set out clear procedures for responding to requests for access to personal information known as subject access requests.
- Report any breaches of the GDPR. Under section 21 of PPC's Standing Orders, responsibility for ensuring compliance with GDPR rests with the Data Protection Officer (DPO) who is the Proper Officer of the Authority.

Conditions for Processing

- The individual has given consent that is specific to the processing activity.
- The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering a contract with the individual, at their request.
- The processing is necessary for the performance of a legal obligation to which we are subject.
- The processing is necessary to protect the vital interests of the individual or another.

Use of Personal Data

PPC collects and uses certain types of personal information about staff, councillors, residents, and other individuals who encounter or communicate with the Council. In each case, the personal data must be treated in accordance with the data protection principles. Any wish to limit or object to the use of personal data should be notified to the DPO in writing. If, in the view of the DPO, the objection cannot be maintained, the individual will be given written reasons why the council cannot comply with their request.

Staff, Councillors, and Volunteers

The personal data held about staff, councillors and volunteers will include contact details, employment history, information relating to career progression, information relating to DBS checks, right to be employed within the UK, and photographs. The data is used to comply with legal obligations placed on PPC in relation to employment. PPC may pass information to other regulatory authorities where appropriate. Personal data will also be used when giving references.

It should be noted that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as “spent” once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

PPC may hold personal information in relation to other individuals who they have contact with such as volunteers. Such information shall be held only in accordance with the data protection principles and shall not be kept longer than necessary.

PPC will take reasonable steps to ensure that members of staff and councillors will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this policy and their duties under the GDPR.

PPC will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

Disclosure of Personal Data to Third Parties

The following list includes the most usual reasons that PPC will authorise disclosure of personal data to a third party:

• To give a confidential reference relating to a current or former employee.

• For the prevention or detection of crime.

• For the assessment of any tax or duty.

• Where it is necessary to exercise a right or obligation conferred or imposed by law upon PPC (other than an obligation imposed by contract).

• For, or in connection with, legal proceedings (including prospective legal proceedings).

• For obtaining legal advice.

PPC may receive requests from third parties to disclose personal data it holds about staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies, or where necessary for the legitimate interests of the individual concerned or PPC.

All requests for the disclosure of personal data must be sent to the DPO, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

Subject Access Requests

Any individual who makes a request to see any personal information held about them by PPC is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure. A subject access request must be made in writing. PPC may ask for any further information reasonably required to locate the information and will require identification to be provided prior to information release.

Other Rights of Individuals

Right to restrict processing
An individual has the right to object to the processing of their personal data and to block or suppress the processing. Where such an objection is made, it must be sent to the DPO who will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings. The DPO shall be responsible for notifying the individual of the outcome of their assessment within 20 working days of receipt of the objection.

Right to rectification
An individual has the right to request the rectification of inaccurate data or incomplete data without undue delay. Where any request for rectification is received, it should be sent to the DPO and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified within 20 days. Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data and communicated to the individual. The individual shall be given details of how to appeal to the Information Commissioner.

An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure
Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

- Where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed.

- Where consent is withdrawn and there is no other legal basis for the processing.

- Where an objection has been raised under the right to object, and there is no overriding legitimate interest for continuing the processing.

- Where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met).

Where the data must be erased to comply with a legal obligation
The DPO will make a decision regarding any application for erasure of personal data and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to object

An individual has the right to object to:

- Processing based upon legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling).

- Direct marketing (including profiling).

- Processing for purposes of scientific /historical research and statistics.

Where such an objection is made, it must be sent to the DPO who will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

The right to lodge a complaint with the Information Commissioner's Office
The Information Commissioner can be contacted on 0303 123 1113 and or via ico.org.uk.

Right to portability
If an individual wants to send their personal data to another organisation they have a right to request that PPC provides their information in a structured, commonly used, and machine readable format. This right is limited to situations where PPC is processing the information based on consent or performance of a contract. If a request for this is made, it should be forwarded to the DPO.

Breach of any Requirements of the GDPR
All breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the DPO. Once notified, the DPO shall assess:

- The extent of the breach.
- The risks to the data subjects because of the breach.
- Any security measures in place that will protect the information.
- Any measures that can be taken immediately to mitigate the risk to the individuals.

Unless the DPO concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of PPC.

The Information Commissioners Office will be told details of the breach, including:

- The volume of data at risk, and the number and categories of data subjects.
- The contact point for any enquiries.
- The likely consequences of the breach.
- The measures proposed or already taken to address the breach.

If the breach is likely to result in a high risk to the affected individuals then the DPO shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Data subjects shall be told:

- The nature of the breach.
- Who to contact with any questions.
- The measures taken to mitigate any risks.

The DPO shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented.

Any recommendations for further training or a change in procedure shall be reviewed by PPC and a decision made about implementation of those recommendations.

February 2026