

Papplewick Parish Council

Data Protection Policy

Purpose and scope	2
Definitions	2
Data protection principles	2
Lawfulness, Fairness and Transparency	3
Purpose limitation (Consent)	3
Data Minimisation	4
Storage Limitation (Records Retention)	4
Integrity and Confidentiality (Security)	4
Accountability (Individual responsibilities)	5
Individual's rights	6
Policy Review	6
Contact and Complaints	6

Purpose and scope

The purpose of this policy is to ensure that employees, councillors and volunteers handling personal information at Papplewick Parish Council (the 'Parish Council') are fully aware of the requirements of the UK General Data Protection Regulations (UK GDPR) and Data Protection Act 2018, and comply with data protection procedures. The policy also aims to ensure that data subjects are aware of their rights.

The aim of this policy is to outline how the Parish Council meets its legal obligations in safeguarding confidentiality and adheres to information security standards.

This policy applies to :

- All councillors, employees, volunteers and contractors who handle personal data on behalf of the Council
- All personal data processed by the Council, whether held in electronic or paper form

Definitions

"Personal data" is any information that relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information. It includes both automated personal data and manual filing systems where personal data are accessible according to specific criteria. It does not include anonymised data.

"Processing" is any use that is made of data, including collecting, recording, organising, consulting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic or biometric data as well as criminal convictions and offences.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

The Parish Council does not process personal data for regular and systematic monitoring of data subjects on a large scale, and it does not process sensitive personal data on a large scale – it has, therefore, not appointed a Data Protection Officer. As a Parish Council, Section 7 (3) (a) of the Data Protection Act 2018 permits this.

Data protection principles

The Parish Council is committed to upholding the data protection principles, which are the fundamental, legally binding rules that dictate how organizations and businesses must collect, handle, and store personal information. Under the UK General Data Protection Regulation (UK GDPR), these principles ensure that personal data is handled responsibly, securely, and transparently.

The seven core data protection principles include:

- **Lawfulness, fairness, and transparency:** Processing must be based on a valid lawful basis (like consent or legal obligation), must not be misleading, and individuals must be clearly informed about how their data is used.

- **Purpose limitation:** Personal data must only be collected for specified, explicit, and legitimate purposes and cannot be used for unrelated reasons later on.
- **Data minimisation:** Organizations should only collect and process the exact amount of personal data that is strictly necessary to fulfil their purpose.
- **Accuracy:** Data must be accurate, kept up to date, and corrected or deleted if it is found to be incorrect
- **Storage limitation:** Personal information must only be kept for as long as is necessary for the purposes for which it was collected
- **Integrity and confidentiality (security):** Data must be protected using appropriate technical and organizational security measures against unauthorized access, loss, or damage
- **Accountability:** Organisations must take responsibility for complying with the principles, keep detailed records, and be able to demonstrate their compliance to regulatory bodies.

Lawfulness, Fairness and Transparency

The council may process personal data for one or more of the following reasons:

- it is necessary for the performance of a contract, e.g., your contract of employment (or services);
- it is necessary to comply with any legal obligation;
- it is necessary for the council's legitimate interests (or for the legitimate interests of a third party), unless there is a good reason to protect your personal data which overrides those legitimate interests;
- it is necessary to protect the vital interests of a data subject or another person;
- it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- It is necessary for a specific reason, other than listed above, and clear consent has been given to use the data.

Purpose limitation (Consent)

Personal data must only be collected for specified, explicit, and legitimate purposes and cannot be used for unrelated reasons later on.

The Parish Council will take all reasonable steps to ensure that service users, members of staff, volunteers, and contractors are informed of the reasons the council requires information from them, how that information will be used and who it will be shared with. This will enable the data subject to give explicit informed consent to the council handling their data where the legal basis for processing is consent.

Should the parish council wish to use personal data for any purpose other than that specified when it was originally obtained, the data subject's explicit consent should be obtained prior to using the data in the new way unless exceptionally such use is in accordance with other provisions of the Act.

Should the parish council wish to share personal data with anyone other than those recipients specified at the time the data was originally obtained, the data subject's explicit consent should be obtained prior to sharing that data, failure to do so could result in a breach of confidentiality.

Data Minimisation

The Parish Council should only collect and process the exact amount of personal data that is strictly necessary to fulfil the purpose for which it is being collected.

If a resident emails a councillor directly with personal information, the policy should mandate that it is immediately forwarded to the Parish Clerk (the official Data Controller) and deleted from the councillor's personal device.

The council should only collect highly specific details when necessary (e.g., PAYE for employees, or contact details for residents who wish to be kept informed on a specific matter).

Storage Limitation (Records Retention)

The Parish Council is committed to ensuring that personal information is only be kept for as long as is necessary for the purposes for which it was collected.

Full details of the Council's GDPR Records Retention Policy can be found on the website.

Integrity and Confidentiality (Security)

The Parish Council takes the security of personal data seriously.

Personal data will be held securely and not available for public access. All data stored by the Parish Clerk is held on a Parish Council PC with password protection.

Where the council engages third parties to process personal data on our behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

International Transfer of Data

Any personal data transferred to countries or territories which do not have equivalent data protection laws to those required in the European Economic Area ("EEA") or United Kingdom, will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts.

Data Protection Impact Assessments (DPIA)

A DPIA is a process which helps to assess privacy risks to individuals in the collection, use and disclosure of information. They must be carried out at the early stages of new projects and be embedded into the council's decision-making process.

Data Breaches

In the event of a suspected data breach, all Councillors and staff have an obligation to report the personal data breach.

- The clerk will notify the council of any breaches immediately.
- The Parish Council is required to report a qualifying data breach to the ICO without delay and within 72 hours after becoming aware of a personal data breach.
- Any / all data breaches will be recorded, along with details of actions taken. This record will help to identify system failures and should be used to improve the security of personal data.

Full details of the Council's Data Breach Policy and Process can be found in the GDPR Data Breach Policy on the website.

Accountability (Individual responsibilities)

The parish council will be responsible for ensuring that the organisation complies with its responsibilities under the Data Protection Act through monitoring of activities and incidents via reporting by the Clerk to the Council. The parish council will also ensure that there are adequate resources to support the work outlined in this policy.

All staff and councillors will ensure that:-

- Personal information is treated in a confidential manner in accordance with this and any associated policies.
- The rights of data subjects are respected at all times.
- Privacy notices will be made available to inform individuals how their data is being processed.
- Personal information is only used for the stated purpose, unless explicit consent has been given by the Data Subject to use their information for a different purpose.
- Personal information is only disclosed on a strict need to know basis, to recipients who are entitled to that information.
- Personal information held within applications, systems, personal or shared drives is only accessed in order to carry out work responsibilities.
- Personal information is recorded accurately and is kept up to date.
- They refer any subject access requests and/or requests in relation to the rights of individuals to the Data Protection Officer.
- They raise actual or potential breaches of the Data Protection Act to the Data Protection Officer as soon as the breach is discovered.

It is the responsibility of all staff and councillors to ensure that they comply with the requirements of this policy and any associated policies or procedures.

Individual's rights

Under UK GDPR legislation, individuals have the following rights in relation to their personal data being processed

- **Right to be Informed:** The right to know what data is collected and how it is used.
- **Right of Access:** Residents can request copies of the personal information the council holds on them (Subject Access Request).
- **Right to Rectification:** The right to demand that inaccurate or incomplete information is corrected.
- **Right to Erasure:** The right to request the deletion of personal data when it is no longer necessary.
- **Right to Restrict or Object:** The right to limit how the council uses your data or to object entirely to its processing.
- **Data Portability:** The right to move, copy, or transfer personal data easily to another IT environment.

Individuals should contact the Clerk to the Council if they would like to exercise any of these rights.

Full details of the Council's GDPR Data Subject Access Request Procedure are available on the website.

As a data subject, you have a number of rights in relation to your personal data.

Policy Review

This policy will be reviewed annually or sooner if required by changes in legislation or the Council's practices.

Contact and Complaints

Questions, concerns or complaints relating to this policy or the Council's Data Protection practices should be directed to the Clerk to the Council (clerk.papplewick@gmail.com)

Individuals also have the right to lodge a complaint with the Information Commissioner's Office (ICO) Website www.ico.org.uk, Telephone 0303 123 1113

Adopted by Papplewick Parish Council 8 July 2026