Drighlington Parish Council

Data Protection Policy

Introduction:

Drighlington Parish Council is regulated in its use of Personal Data under the Data Protection Act 2018 and the General Data Protection Regulation.

The Parish Council holds Personal Data about its councillors, employees, members of the public, suppliers, contractors and other individuals, for a variety of council purposes.

This policy sets out how the Parish Council seeks to protect Personal Data and ensure that councillors and the clerk understand the rules governing its use. This policy requires the clerk to consider data protection legislation and best practice before any significant new data processing activity is initiated, to ensure that relevant compliance steps are addressed.

This policy should be read in conjunction with Drighlington Parish Council's IT Policy.

Scope:

This policy applies to all councillors and staff. Councillors and staff must be familiar with this policy and comply with its terms.

Definitions:

The General Data Protection Regulation: "The GDPR" Regulation (EU) 2016/679 of the European Parliament and the Council of 27th April 2016 on the protection of natural persons concerning the processing of personal data and on the free movement of such data.

The Data Protection Legislation: The Data Protection Act 2018 and the GDPR.

Personal Data: Any information relating to an identified or identifiable living individual.

Data Subject: An individual about whom personal data is held. It does not include anyone who has died, or who cannot be identified or distinguished from others.

Processing Data: Processing in relation to information means an operation or set of operations which is performed on information, or on sets of information, such as:

- a) collection, recording, organisation, structuring or storage,
- b) adaptation or alteration,
- c) retrieval, consultation, or use,
- d) disclosure by transmission, dissemination or otherwise making available,
- e) alignment or combination, or
- f) restriction, erasure, or destruction

Sensitive Personal Data: Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data, or of biometric data, for uniquely identifying an individual; data concerning health; or data concerning an individual's sex life or sexual orientation. Data relating to criminal offences will be treated as Sensitive Personal Data.

Council Purposes: The purposes for which Personal Data may be used by the Parish Council. Parish Council purposes include the following:

- a) Compliance with legal, regulatory, and corporate governance obligations and good practice
- b) Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests.
- c) Ensuring the Parish Council policies are adhered to (such as policies covering email and internet use)
- d) Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of sensitive information, securing vetting and checking.
- e) Investigating complaints
- f) Ensuring safe working practices, general administration, payroll, and providing access to systems and facilities.

Data Protection Officer:

Under the Data Protection Act 2018, public authorities are required to appoint a Data Protection Officer. However, the provisions of section 7 (3)(a) of the Act remove Parish Councils from this requirement.

Data Controller/Data Processor:

The Parish Council is the Data Controller. The Clerk to the Council is the Data Processor Officer and has the overall responsibility for the day-to-day implementation of this Policy. Responsibilities of the Data Processor Officer:

- a) Keeping the Parish Council updated about data protection responsibilities, risks and issues.
- b) Reviewing all data protection procedures and policies regularly.
- c) Assisting with data protection training.
- d) Answering questions on data protection from staff, council members, members of the public and other stakeholders.
- e) Responding to individuals such as members of the public, service users and employees who wish to know which data is being held on them.
- f) Checking and approving with third parties that handle the council's data contracts or agreements regarding data processing.
- g) Ensure all systems, services, software and equipment meet acceptable security standards.
- Being the primary contact.

Procedures:

Collecting Data

The Parish Council will ensure any collection and use of Personal Data is justified under at least one of the conditions for processing:

1 Consent – the data subject has consented to the processing. This may be revoked at any time.

2 Contractual – it is necessary in relation to a contract that the data subject has entered into or wishes to enter into.

3 Legal obligation – it is necessary because of a legal obligation, other than contractual.

4 Vital interests – it is a “life or death” matter for the Data Subject.

5 Public tasks – it is necessary for administering, or for exercising statutory.

6 Legitimate interests – Processing is lawful when no other lawful bases apply, but requires an additional risk assessment. The data can only be collected if it passes the additional risk assessment.

Data Protection Principles:

Drighlington Parish Council will process personal data in compliance with all six data protection principles:

1. **Lawfulness, fairness and transparency**
   It will make sure that its data collection practices don’t break the law and that it isn’t hiding anything from data subjects.
2. **Purpose limitation**
   It will only collect personal data for a specific purpose, clearly state what that purpose is, and only collect data for as long as necessary to complete that purpose.
3. **Data minimisation**
   It will only process the personal data that it needs to achieve its processing purposes.
4. **Accuracy**
   It will take all reasonable steps to erase or rectify data that is inaccurate or incomplete.
5. **Storage limitation**
   It will delete personal data when it is no longer necessary.
6. **Integrity and confidentiality**
   It will ensure appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

P**rivacy Notices:**

To demonstrate transparency and provide accessible information to individuals about how it will use Personal Data, when information is being collected, the Parish Council will provide a privacy notice.

Sensitive Personal Data:

The Parish Council will document the additional justification for the processing of sensitive data. In most cases where the Council processes Sensitive Personal Data, it will require the data subject’s explicit consent to do this unless exceptional circumstances apply, or where the Parish Council is required to do this. Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and Relevance:

The Parish Council will ensure that any personal data it processes is accurate, adequate, relevant, and not excessive, given the purpose for which it was obtained. The Parish Council will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this. A data subject may ask for inaccurate personal data relating to them to be corrected. This should be reported to the Data Processor Officer.

Councillors' Personal Data:

Councillors must take reasonable steps to ensure that personal data the Parish Council holds about them is accurate and updated as required.

Data Security:

Personal data must be kept secure against loss or misuse. Where other organisations process personal data as a service on the Parish Council's behalf, the clerk will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing data securely:

- a) In cases when data is stored on printed paper, it will be kept in a secure place where unauthorised personnel cannot access it.
- b) Printed data will be shredded when it is no longer needed.
- c) Date stored on a computer will be protected by strong passwords that are changed regularly.
- d) Data stored on CDs or memory sticks will be similarly password-protected.
- e) Data will be regularly backed up in line with the council's backup procedures.
- g) Data must never be saved directly onto unprotected mobile devices such as tablets or smartphones.
- h) All servers containing sensitive data must be approved and protected by security software and a strong firewall.

Data Retention:

The Parish Council must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained.

Subject Access Requests and data portability:

A Data Subject is entitled, subject to certain exceptions, to request access to information held about them in a structured format. All Subject Access Requests must immediately be referred to the clerk, who will process the requests within the legal timescale, provided there is no undue burden, and it does not compromise the privacy of other individuals. A Data Subject may also request that their data be transferred directly to another system.

Right to be Forgotten:

A Data Subject may request that any information held on them be deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Review:

The Parish Council will review the policy annually.

Policy Details / Version History

Date First Adopted: 16 March 2026 **Minute Reference:** 745/26
Document Status: Adopted
Review Period: