Rollesby Parish Council

Data Protection Policy

Introduction

Rollesby 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, residents, suppliers, 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.

Definitions

The General Data Protection Regulation "The GDPR"

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to 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.

Data Protection Officer

Data Protection Legislation requires certain public authorities and data processors to appoint a Data Protection Officer (DPO).

The role of the DPO is to assist the monitoring of internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for Data Subjects and the Supervisory Authority.

Data Controller

Person who determines the purpose and means of the processing of Personal Data

Data Processor

Person who processes the data on behalf of the Data Controller.

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 the purpose of 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.

Council Purposes include the following:

- Compliance with legal, regulatory, and corporate governance obligations and good practice

- Gathering information as part of investigations by regulatory bodies or in connection with legal
- proceedings or requests
- Ensuring council policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions, training, and quality control, ensuring the confidentiality of sensitive information, security vetting and checking
- The management and operation of the Council's cemetery, CCTV, allotments, and farm tenancies.
- Investigating complaints
- Ensuring safe working practices, general administration, payroll, providing access to systems and facilities.

Scope

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

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

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 removes Parish Council's from this requirement. Rollesby Parish Council have not appointed a Data Protection Officer.

Data Controller

The Clerk is the Data Controller and has overall responsibility for the day-to-day implementation of this policy.

The Clerk, 58 Hercules Road, Hellesdon, Norwich, Norfolk, NR6 5HH. Email: rollesbypc@gmail.com telephone: 07340028540

The Clerk will receive appropriate training, as required.

Responsibilities of the Data Controller

- Keeping the Council updated about data protection responsibilities, risks, and issues
- Reviewing all data protection procedures and policies on a regular basis
- Assisting with data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, council members and other stakeholders
- Responding to individuals such as members of the public, service users and employees who wish to know which data is being held on them by Rollesby.
- Checking and approving with third parties that handle the council's data any contracts or agreement regarding data processing
- Ensure all systems, services, software, and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data
- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

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 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 justice, or for exercising statutory, governmental, or other public function.
6. Legitimate interests - it is necessary for the organisation's legitimate interest or those of a third party to whom the personal data is disclosed, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Data protection principles

The 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.

Privacy 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 two types of privacy notice:

1. To staff members, councillors, contractors, and anyone else with a role in the council.
2. To residents and members of the public.

In each instance the privacy notice will detail:

- What information is being collected.
- Who is collecting the information.
- How the information is being collected.
- Why the information is being collected.
- How the information will be used.
- Who the information might be shared with.
- The right of access to personal data that the Parish Council holds about them.
- The identity and contact details of any data controllers.
- The retention period for the information.
- The conditions for processing.

Sensitive Personal Data

The Parish Council will document the additional justification for the processing of sensitive data.

In most cases where the Parish 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 by. 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.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

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 DPO.

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

- In cases when data is stored on printed paper, it will be kept in a secure place where unauthorized personnel cannot access it
- Printed data will be shredded when it is no longer needed
- Data stored on a computer will be protected by strong passwords that are changed regularly. The Parish Council encourage councillors and staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks will be similarly password protected.
- The Clerk must approve any cloud used to store data
- Data will be regularly backed up in line with the council's backup procedures
- Data must never be saved directly onto unprotected mobile devices such tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and 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. It should be determined in a manner consistent with our data retention guidelines.

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 one month, 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 is transferred directly to another system. This will be done free of charge.

Right to be forgotten

A Data Subject may request that any information held on them is 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.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Clerk will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All Councillors and members of staff have an obligation to report actual or potential data protection compliance failures. This allows the Parish Council to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

Please refer to the Parish Council's Compliance Failure Policy for the reporting procedure.

Monitoring

The Clerk will monitor the policy regularly to ensure that it is being adhered to.

Consequences of failing to comply

The Parish Council takes compliance with this policy very seriously. Failure to comply puts both the individual and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action.

Any questions or concerns about anything in this policy, do not hesitate to contact the clerk.