Rooksdown Parish Council

Empowering our community

Data Protection Policy

September 2018 v1.0 as approved

1 Introduction

Rooksdown Parish Council (RPC) is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with our legal obligations.

We hold personal data about officers, councillors, suppliers, residents and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that officers and councillors understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires officers and councillors to ensure that the Data Control Committee be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Appendix A gives examples of processes that must be undertaken by officers and councillors to conform with this Policy.

2 Definitions

(Explanatory notes are in italics below)

Business purposes	purposes for which data is processed by RPC, including personnel, administrative, financial, regulatory, payroll and communication with the public *Business purposes include the following:* - *Compliance with our 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 business 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 commercially sensitive information, security vetting, credit scoring and checking* - *Investigating complaints* - *Checking references, ensuring safe working practices, monitoring and managing access to systems and facilities and staff absences, administration and assessments* - *Monitoring officer and councillor conduct, disciplinary matters* - *Marketing our business* - *Improving services*
Personal data	information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person *Personal data we gather may include: individuals' phone number, email address, address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.*
Special categories of personal data	information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health

	or condition, criminal offences, or related proceedings, and genetic and biometric information *Any use of special categories of personal data should be strictly controlled in accordance with this policy.*
Data controller	natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.
Data processor	natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Material personal data breach	breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, whether accidental or deliberate, that poses a significant risk to a person's rights or freedoms.
Processing	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3 Scope

This policy applies to all officers and councillors, who must be familiar with this policy and comply with its terms.

This policy supplements any other policies relating to internet and email use. RPC may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will need to be approved formally by RPC.

3.1 Who is responsible for this policy?

The RPC Data Control Committee (DCC) as the Data Controller is responsible for setting this policy. All officers and councillors are responsible for implementation of this policy.

4 The principles

RPC shall comply with the principles of data protection (the Principles) enumerated in the General Data Protection Regulations (GDPR).

The Principles are:

1. **Lawful, fair and transparent**

   Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2. **Limited to its purpose**

   Data can only be collected for a specific purpose.

3. **Data minimisation**

   Any data collected must be necessary and not excessive for its purpose.

4. **Accurate**

   The data we hold must be accurate and kept up to date.

5. **Retention**

   We cannot store data longer than necessary for the purpose for which it was collected.

6. **Integrity and confidentiality**

The data we hold must be kept safe and secure.

4.1 Accountability and transparency

We must ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle. The DCC is responsible for ensuring that all data processing activities comply with each of the Principles.

To comply with data protection laws and the accountability and transparency Principle of GDPR, we must demonstrate compliance. Officers and councillors are responsible for understanding their particular responsibilities to ensure we meet the following data protection obligations:

- To fully implement all appropriate technical and organisational measures
- To maintain up to date and relevant documentation on all processing activities
- To implement measures to ensure privacy by design and default, including:
  - Data minimisation
  - Pseudonymisation
  - Transparency
  - Allowing individuals to monitor processing
  - Creating and improving security and enhanced privacy procedures on an ongoing basis.

5 Our procedures

5.1 Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should only process personal data if there is a lawful basis (explained below) for so doing.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

5.2 Controlling vs. processing data

RPC is classified as a data controller and a data processor. We must maintain our appropriate registration with the Information Commissioners Office (ICO) to continue lawfully controlling and processing data.

Councillors and officers are all data processors.

As a data processor, we must act only on the documented instructions of the data controller. If we at any point determine the purpose and means of processing outwith the instructions of the controller, we shall be considered a data controller and therefore breach our contract with the controller and have the same liability as the controller. As a data processor, we must:

- Not use a sub-processor without written authorisation of the data controller
- Co-operate fully with the ICO
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches

If officers and councillors are in any doubt about how data should be handled, contact the Clerk for clarification.

5.3 Lawful basis for processing data

We must establish a lawful basis for processing data. Officers and councillors must ensure that any data they process has a lawful basis approved by the DCC. It is the individual's responsibility to check the lawful basis for processing any data they are working with and ensure all their actions comply with the lawful basis. At least one of the following conditions must apply whenever we process personal data:

1. **Consent**

   We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

2. **Contract**

   The processing is necessary to fulfil or prepare a contract for the individual.

3. **Legal obligation**

   We have a legal obligation to process the data (other than a contract).

4. **Vital interests**

   Processing the data is necessary to protect a person's life or wellbeing.

5. **Public function**

   Processing is necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. **Legitimate interest**

   The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

5.4 Deciding which condition to rely on

If officers and councillors are making an assessment of the lawful basis, they must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. Officers and councillors cannot rely on a lawful basis if they can reasonably achieve the same purpose by some other means.

Officers and councillors must remember that more than one basis may apply, and they should rely on what will best fit the purpose, not what is easiest.

To decide on which conditions apply, consider the following factors:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

If officers and councillors are responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, they must have this approved by the DCC.

6 Special categories of personal data

6.1 What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

In most cases where we process special categories of personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). 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.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

7 Responsibilities

7.1 Our responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identifying the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Storing data in safe and secure ways
- Assessing the risk that could be posed to individual rights and freedoms should data be compromised

7.2 Officers' and councillors' responsibilities

- To fully understand data protection obligations
- To check that any data processing activities undertaken by them comply with our policy and are justified
- Not to use data in any unlawful way
- Not to store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through their actions
- Comply with this policy at all times
- Raise any concerns, notify any material personal data breach or error, and report anything suspicious or contradictory to this policy or our legal obligations without delay.

7.3 Responsibilities of the Data Controller (the DCC)

- Ensuring that
  - all systems, services, software and equipment meet acceptable security standards
  - third-party services, such as cloud services RPC is considering using to store or process data, meet GDPR requirements
- 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 DCC to ensure all marketing initiatives adhere to data protection laws and RPC's Data Protection Policy.

7.4 Accuracy and relevance

Officers and councillors will ensure that any personal data they process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. Officers and councillors 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.

Individuals may ask that inaccurate personal data relating to them is corrected. If officers and councillors believe that information is inaccurate they should inform the Clerk or the DCC.

7.5 Data security

Officers and councillors must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DCC will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

7.6 Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should be shredded when it is no longer needed.
- Data stored on a computer or in the cloud should be protected by strong passwords. We encourage all officers and councillors to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used.
- Servers containing personal data must be kept in a secure location, away from general office space.
- Data should be regularly backed up in line with RPC's backup procedures.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones, unless it is deleted immediately after being processed.
- All reasonable technical measures must be put in place to keep data secure.

7.7 Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

7.8 Transferring data internationally

There are restrictions on international transfers of personal data. Officers and councillors must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the DCC.

8 Rights of individuals

Individuals have rights to their data which officers and councillors must respect and comply with to the best of our ability. Officers and councillors must ensure individuals can exercise their rights in the following ways:

1. **Right to be informed**
    - Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
    - Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.
2. **Right of access**
    - Enabling individuals to access their personal data and supplementary information

- Allowing individuals to be aware of and verify the lawfulness of the processing activities

3. **Right to rectification**
    - Officers and councillors must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
    - This must be done within 1 month of notification.
4. **Right to erasure**
    - Officers and councillors must delete or remove an individual's data if requested and there is no remaining lawful basis for its continued processing.
5. **Right to restrict processing**
    - Officers and councillors must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
    - Officers and councillors are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.
6. **Right to data portability**
    - Officers and councillors must provide individuals with their data so that they can reuse it for their own purposes or across different services.
    - Officers and councillors must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.
7. **Right to object**
    - Officers and councillors must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
    - Officers and councillors must respect the right of an individual to object to direct marketing.
    - Officers and councillors must respect the right of an individual to object to processing their data for scientific and historical research and statistics.
8. **Rights in relation to automated decision making and profiling**
    - Officers and councillors must respect the rights of individuals in relation to automated decision making.
    - Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

9 Privacy notices

9.1 When to supply a privacy notice

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which means within one month.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

9.2 What to include in a privacy notice

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children.

The following information must be included in a privacy notice to all data subjects:

- Identification and contact information of the data controller
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- Detailed information of any transfers to third countries and safeguards in place
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and internal complaint procedures
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
- Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

10 Subject Access Requests

10.1 What is a subject access request?

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a privacy notice.

10.2 How we deal with subject access requests

We must provide an individual with a copy of the information the request, free of charge. This must occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the reason for requesting the information.

Once a subject access request has been made, the data must not be changed or amended in any way. Doing so is a criminal offence.

10.3 Data portability requests

We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to them. This must be done free of charge and without delay, and no later than one month. The information will normally be provided by the Clerk unless it involves data held on systems only accessible to other officers or councillors. For complex or numerous requests the response period can be extended to two months with the approval of the Clerk, but the individual must be informed of the extension within one month and the DCC must be informed.

11 Right to erasure

11.1 What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn

- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

11.2 How we deal with the right to erasure

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

11.3 The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. officers and councillors must cease processing unless:

- There are legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online or by email.

11.4 The right to restrict automated profiling or decision making

We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, we must:

- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

12 Third parties

Using third party controllers and processors:

- As a data controller and data processor, we must have written contracts in place with any third-party data controllers and/or data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.
- As a data controller, we must only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.
- As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

12.1 Contracts

Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with data controllers and/or data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

- The recipient must act only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of material personal data breach and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on GDPR.

13 Criminal offence data

13.1 Criminal record checks

Any criminal record checks must be justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. The DCC must give approval prior to carrying out a criminal record check.

14 Audits, monitoring and training

14.1 Data audits

We must perform regular data audits to manage and mitigate risks and 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. The DCC may authorise an audit at any time.

14.2 Monitoring

The DCC has overall responsibility for this policy and will keep this policy under review and amend or change it as required. Officers and councillors must comply with this policy fully and at all times.

14.3 Training

Officers and councillors will receive adequate training on provisions of data protection law specific for their role. If additional training is required, the Clerk should be informed.

15 Reporting material personal data breaches

Any material personal data breach or of data protection laws must be reported as soon as practically possible. This means as soon as officers and councillors become aware of a breach. RPC has a legal obligation to report significant data breaches – ie those involving potential significant harm to the rights of individuals - to the ICO within 72 hours.

All officers and councillors have an obligation to report actual or potential data protection compliance failures. This allows us to:

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

Any officer or councillor who fails to notify of a material personal data breach or is found to have known or suspected a material personal data breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Any breaches must be reported immediately to the Clerk and the Chairman of the DCC.

15.1 Failure to comply

RPC takes compliance with this policy very seriously. Failure to comply puts individuals and the organisation at risk.

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

Appendix A – Example Processes

Below are examples of processes that must be undertaken by officers and councillors and officers to conform with this Policy.

1. Paper records, eg for allotment applicants, must be kept in a locked filing cabinet when not in use.
2. Councillors may copy information from Office 365 on to personal laptops, tablets, phones or PCs but all information must be deleted when processing is finished.
3. All data should be deleted in accordance with RPC's retention policy [to be added]
4. Information collected for one purpose (eg allotment application) must not be used for another (eg a newsletter) without the subject's consent.

[List to be completed]