



Rayne Parish Council

Subject Access Request Policy

1. Introduction and policy statement

1.1 As a Data Controller, Rayne Parish Council (RPC) processes personal data about residents, service users, staff, customers and/or their families in records of a number of services. Such persons for the purpose of the Act are Data Subjects and entitled to certain rights.

1.2 The Data Protection Act and the General Data Protection Regulations (the Act) provide Data Subjects the right, subject to certain exceptions, to view and or obtain a copy of all personal data that a Data Controller holds about them.

1.3 These requests are known as Subject Access Requests (SARs) and apply to personal information relating to living individuals held in computerised or manual formats irrespective of when they were created.

1.4 RPC has a statutory duty to comply with the Act to enable individuals to find out and see what personal data is held about them, why it is being held and who it is shared with. The aim of this policy is to ensure RPC provides subject access in accordance with the law and good practice.

1.5 This policy sets out how RPC will support the exercise of the right of access and ensures that staff are aware of their responsibilities in recognising, handling and processing SARs.

2. Definitions

2.1 Data Controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is, or is to be, processed. The Data Controller is Rayne Parish Council.

2.2 Parental Responsibility

Parental responsibility is defined in the Children Act 1998 as 'all the rights, duties, powers, responsibilities and authority which by law a parent of a child has in relation to the child and his property'. A person with parental responsibility is defined in law and by reference to the circumstances of each child and any legal proceedings or lawful processes affecting persons who may be in a parental role for that child. A reference list is set out in the appendix.

2.3 Personal Data

Data which relates to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the

individual and any indication of the intentions of the data controller or any other person in respect of the individual.

2.4 Subject Access

The right of a Data Subject to have access to their own personal data

3. Roles & Responsibilities

3.1. Data Protection Officer

The Data Protection Officer holds overall responsibility for Subject Access Requests throughout RPC, but on a day-to-day basis this will be delegated to:

- the Parish Council Clerk

3.2. the Parish Council Clerk is responsible for:

Co-ordinating subject access requests while ensuring they are responded to correctly in accordance with statutory requirements.

Locating all relevant information relating to the request.

Ensuring that the personal data is checked to see if the record contains information relating to another individual, or information provided by a third party, who can be identified from the entry and unless that person has consented to disclosure, deciding on and making appropriate redaction of the data.

Acting as a reference point for procedures and complaints as detailed in this policy.

Alerting the Data Protection Officer to problems that affect the carrying out of the process.

Ensuring action is taken in response to any relevant post-access enquiries regarding data accuracy or other relevant enquiries.

3.3 RPC Staff responsibilities:

Any member of staff or councillor receiving a SAR should forward this immediately to the Parish Council Clerk.

They are then responsible for supporting the process and will:

- Provide an appropriate point of contact for the Data Subject during the Subject Access process.
- Co-ordinate the retrieval of data.
- Ensure timescales are met.
- Facilitate the retrieval of data whether its paper or electronic.
- Seek general advice from the DPO when necessary.

- Collect material for disclosure, check the records and redact third party data where required.
- Contribute to final judgements about which data items should be withheld from disclosure following consultation with the DPO.

4. Children under 18 years

4.1 Even if a child is too young to understand the implications of subject access rights, data about them is still their personal data and does not belong to anyone else, such as a parent or guardian. In the case of young children these rights are likely to be exercised by those with parental responsibility for them. Where an adult requests a child's data, proof of parental responsibility will be required. Officers should be alert to any situation where there may be a conflict between different persons who hold parental responsibility in relation to the child.

4.2 Before responding to a SAR for information held about a child, we will consider whether the child is mature enough to understand their rights. Normally a child is deemed to understand a request from the age of 12 years. If they are considered to be so competent we will respond to or consult the child or seek the child's consent for disclosure to the person with parental responsibility who is making the request or supporting it.

5. Solicitors or Insurance Companies or Agent or Attorney

5.1 Where a legal, financial or other professional or company requests access on behalf of a client they are representing, they must provide the signed consent of their client. The request will be dealt with in the same way as if it had come direct from the client or represented person. We will rely on the legal representative or insurance company to obtain proof of identity of their client. Checks will be made where appropriate when a SAR is made by an agent on behalf of the Data Subject. The Data Subject's signed consent will be required. We may still check with the Data Subject whether he or she is happy with the agent receiving the personal data and should explain the implications of the request. If there is reasonable doubt about the validity of the consent, the request will not be processed until we are satisfied that it is a valid request. Where a request is made by a person acting under a Power of Attorney a copy of the signed and valid document creating the power will be required.

6 Access on Behalf of a Mentally Incapacitated Adult

6.1 Where an individual or an organisation submits a Subject Access Request on behalf of a vulnerable person who lacks capacity, care will be taken to ensure there is an appropriate authority in place such as a valid power of attorney or court order.

7. Access to the Personal Data of Deceased Individuals.

7.1 The subject access right relates to personal data of living individuals. The data of deceased individuals is governed by the Freedom of Information Act 2000. This does not mean that personal data of deceased individuals can be automatically passed into the public domain. The deceased's data is likely to be confidential and the deceased's next of kin as the custodian of the deceased's right to confidentiality. We will have regard to any duty of confidentiality owed to the deceased or to the next of kin or their estate.

8. The Procedure

Formalities

8.1 Applications should be made in writing. This can be via email, fax or social media. If there is reasonable doubt about the validity of the request we will not process it until we are satisfied that it is valid.

8.2 We will make appropriate reasonable adjustments to support the process for any person with a disability or difficulty in making a SAR by all reasonable measures such as treating a verbal request for information as though it were a valid SAR or providing information in an accessible format.

8.3 In order to ensure disclosure is effected to the person who is entitled to it all applicants must provide two forms of identity one of which must be a photo ID such as a passport or driving licence and the other a recent utility bill or similar of not more than three months old. We do not require original documents provided we receive good quality or certified copies.

8.4 Receipt of a SAR will be acknowledged in writing and the Data Subject or requesting person will be provided with a completion date.

8.5 The statutory time period for compliance is calculated from receipt of a valid request. The period is one calendar month, which can be extended by a further two months where requests are complex or numerous. If we decide to extend the time period we will inform the individual within one month of the receipt of the request and explain why the extension is necessary. The time limit will not begin until all identification and any relevant consent is received, any appropriate fee is received and clarification, if required, as to what is being requested is received.

8.6 There is no charge for this service.

Location and preparation of information for disclosure

8.7 All paper files, email systems and electronic data bases and storage will be considered during data retrieval, as all or any may contain personal data of the customer or member of staff.

8.8 Data must be prepared to ensure only appropriate data is disclosed. The process of identifying and removing non-disclosable data is known as redaction and may be performed using specialist software. In relation to the Subject Access process, this means the removal of third party personal data recorded on requested records. We will not disclose third party data without the consent of that individual.

8.9 Sometimes third party data cannot be redacted because it is inextricably linked with that of the data subject and in that case we will not disclose that part of the record unless it is fair in all the circumstances to do so. We will seek permission of the data subject to contact the relevant third party for consent.

8.10 A professional opinion about the data subject is their personal information and must be released except where any exemptions apply. Information about the person that has been received from a relevant professional may often represent that professional's opinion. You should consider whether to redact their name and business contact details. You should carefully consider any objections a professional makes to the disclosure of these details. This is especially important if there is a real risk that disclosure of this information would be likely to cause them, or any other individual, harm. If you suspect the disclosure of it will cause specific problems, you may wish to seek the views of the named relevant professionals about it. You should explain clearly that, if they object to the disclosure of all or part of any data, that this must be based on one of the relevant exemptions [see below]. You should also explain that, whilst you will consider their views, the final decision about disclosure rests with the Parish Council as the Data Controller.

8.11 Permission will be sought from the data subject if we need to contact other individuals about whom personal information is recorded on their file. If permission is given we will then seek the individual's consent to share their data with the data subject. This may include family members and friends. We may rely upon the data subject to supply us with up-to-date contact details for these people. If current contact details cannot be supplied, contact the Parish Clerk who may be able to trace the relevant people or to advise on the relevance to the data subject of doing so. The data subject has the right to request that we do not contact certain individuals. For instance, a child considered to be competent to do so, might not want us to contact their parents. If this is the case we will comply with that instruction and the data subject should be informed that some of the data may be redacted prior to the release of their records.

8.12 Any paper files required for the request will be scanned, all files will be returned to the point of origin. The document is then converted so specialist software can be used on the document. A log is kept of all files requested. The Parish Council Clerk will then consider the document for data of any third parties or any exemptions that may apply.

Disclosure of information and completing the SAR

8.13 Records are usually disclosed electronically by sending a password protected timed encrypted link by email to download the data. The link will expire after five working days.

8.14 Records can be sent by encrypted email if requested and if the size of the files allows. If a paper copy is requested, arrangements will be made with the data subject as to how we can securely deliver the records to them. This may be by hand delivery, courier or special tracked delivery. If it is by hand delivery or collection, identification of the correct recipient will be required.

8.15 A Data Subject has the right to have personal data communicated to him or her in an intelligible manner. If the Data Subject cannot clearly understand instances of data, we will explain the data.

8.16 A record of the request, its current status and completion will be recorded in an electronic system for legal and statistical purposes.

9. Denial of Access

Access to all or part of a record will be denied if:

9.1 It is third party data. Unless the third party is an education, health or social services professional where the information should be regarded as provided by a 'relevant professional' and not a 'third party'.

9.2 The record contains third party data which cannot be redacted because it is inextricably linked with that of the data subject and it would not be reasonable in all the circumstances to disclose it without the consent of the third party and such consent cannot be secured or is withheld.

9.3 The record contains data of a deceased person where disclosure would breach the duty of confidentiality owed to the deceased or their next of kin or estate.

9.4 Disclosure would be likely to cause serious harm to the physical or mental health of the applicant or another person.

9.5 Disclosure would be likely to prejudice the carrying out of social work by reason of the fact that serious harm to the physical or mental health or condition of the data subject or any other person would be likely to be caused.

9.6 Data is processed for any criminal investigation or procedure or taxation purposes where the provision of this information would be likely to prejudice that purpose.

9.7 Data is processed for the purposes of national security.

9.8 The request is an identical or similar request to one already dealt with, unless a reasonable interval has elapsed between the earlier request and the current one.

9.9 The record consists of information for which legal professional privilege could be claimed in legal proceedings in any part of the UK.

9.10 The record is the subject of regulatory activity as defined by the Act and disclosure would be likely to prejudice that investigation.

10. Complaints Procedure

10.1 The data subject or requesting person shall be informed that, if they have any query or disagreement with any decisions made regarding a SAR including the information provided, he or she should contact the DPO.

Appendix

List of persons who will hold parental responsibility for a child:-

the natural mother;

the natural father, if married to the mother either before or after the birth, even if divorced or separated;

the natural father, if unmarried, and he registered the birth along with the mother from 1 December 2003 and therefore is named on the child's birth certificate;

the natural father, if unmarried, by agreement with the mother (evidenced by a form provided by a solicitor, signed by both parents and witnessed by an Officer of the Court) or by a court order (parental responsibility order);

the natural father, if unmarried, and appointed as the child's guardian on the death of the natural mother;

Same-sex partners will both have parental responsibility if they were civil partners at the time of the treatment, e.g. donor insemination or fertility treatment.

Same-sex partners who aren't civil partners - the second parent may acquire parental responsibility by either:

- court order or by making a parental responsibility agreement
- becoming a civil partner of the other parent and making a parental responsibility agreement or jointly registering the birth

an individual with a residence order for the child. An individual who has legally adopted the child;

an individual who has a Special Guardianship Order for the child a local authority under a care order a person who has an emergency Protection Order.

Date Effective From: March 2018

Last Review Date: January 2023

Next Review Date: January 2024