Policy for compliance with GDPR.

1. Introduction.

This policy describes measures introduced to comply with the General Data Protection Regulation.

2. Exclusions.

The Parish Council will not undertake any of the following activities without revision of its polices to include compliant procedures.

- Holding personal data that relies on "consent".
- Using CCTV.
- Holding personal data on children.
- Holding "sensitive" data.
- Allowing third party processing of data.
- Appointing a Data Protection Officer. (this earlier requirement having been removed)
- Undertaking projects requiring a Data Protection impact assessment.

3. Data audit.

The Parish Council will maintain a Data Audit identifying data processed and the legal basis for doing so. This data audit is appended to this policy (APPENDIX 1) and will be reviewed annually at the same time as the policy.

4. Privacy Policy.

The Parish Council will maintain a separate Privacy Policy outlining a range of possible data collection and processing activities that might be undertaken. A link to this policy on the Parish Council's website will be included in all Parish Council correspondence. (Paper and electronic).

5. Data security.

The following apply to the Clerk and Councillors unless otherwise specified.
The effect must be that no one outside the Council can easily gain access to Council information.

- **E-mail.**
  Separate e-mail accounts will be used for Parish Council e-mail. These will be protected by a unique password.

- **Downloaded or original electronic documents containing personal data.**
  Any media on which these are stored (Computer hard drive, external hard drive, memory stick or mobile device) should be protected by a unique password.

- **Paper documents containing personal data.**
  These must be stored securely.

Councillors will be asked to confirm that they have understood and complied with these requirements. The Clerk will keep a record of this confirmation.

6. Website.

No new personal data will be placed on parts of the Parish Council website accessible by the public. (e.g. in agendas, minutes, reports, calendars, forms or other documents).

7. Data retention

Councillors should not retain electronic data (e mail, documents) or paper documents for more than two years.

(note that this is to simplify the management of data retention for Councilors. It will, for example, still allow retention of successive years' budgets for comparison. Documents that may be of use after two years are still likely to he retained by the Clerk so can be made available on request. Documents placed on the website (minutes, agendas, policies, annual reports) will still be accessible.)

Paper and electronic data older than ten years will be reviewed annually by the Clerk and either

- destroyed
- retained as being of potential practical benefit subject to further review
- retained as a historic archive

All minutes, agendas and accounts in existence at the time of implementation of the policy will be treated as archived material.

(note that it is considered necessary to simplify the management of data retention by the Clerk in this manner in order to avoid the use of a level of public resource that would be manifestly disproportionate to the public interest served.)

8. Termination of office

Councillors should not retain any data after ceasing to be in office.

On the appointment of a new Clerk all Council data will be released by the former Clerk and made available to the new Clerk. No data should be retained other than data personal to the outgoing Clerk.

9. Subject Access requests

Responses to Subject Access Requests will be dealt with using the model steps provided by the Derbyshire Association of Local Councils (APPENDIX 2).

10. Security Breaches

A data breech occurs when personal data is accessed (or could have been accessed) by someone for whom it was not intended.

The Clerk or Councilors may become aware of potential security breach themselves, or it may be raised by a third party. If either happens it should be assessed by the Data Controller (Clerk) using the Example Data Breach Assessment Checklist provided by the Derbyshire Association of Local Councils (APPENDIX 3).

The assessment will be used to determine the appropriate course of action in line with GDPR requirements which can be found here

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

(or elsewhere in the Information Commissioner's Office website).

(Note that this may include informing the individual whose data has been compromised and informing the ICO within 72 hours).

Parwich Parish Council

GDPR Policy. APPENDIX 1. Data Audit

Parwich Parish Council Data Audit

Description	What personal information is collected	Why is the data held and what is it used for	Basis for processing data (1)	Who holds the data and who can access it?	What security controls are in place? (2)	How long is data kept for? (3)	Is this covered by our privacy notice? (4)	ACTION REQUIRED
Correspondence with residents	Names, contact details, views, requests	Responding to enquiries, requesting information or action	Public task, Legitimate interest	Held by Clerk, contained in e-mails copied to Councillors	Paper copies secured. Electronic copies require password to access.	No longer than ten years unless archived	Yes	Write and Implement policy
Correspondence with potential suppliers	Names, contact details responses	Tendering	Public task	Held by Clerk, contained in e-mails copied to Councillors	Paper copies secured. Electronic copies require password to access.	No longer than ten years unless archived	Yes	Write and Implement policy
Correspondence with suppliers	Names, contact detail, contracts, arrangements	Tendering for, placemnet of and payment for goods and services	Contract	Held by Clerk, contained in e-mails copied to Councillors	Paper copies secured. Electronic copies require password to access.	No longer than ten years unless archived	Yes	Write and Implement policy
Correspondence with tenants	Names, contact details, agreements, invoicing	Tenancy agreements, payments and issues arising	Contract	Held by Clerk, contained in e-mails copied to Councillors	Paper copies secured. Electronic copies require password to access.	No longer than ten years unless archived	Yes	Write and Implement policy
Correspondence with external bodies (e.g. DCC, HMRC, DALC)	Names, contact details, various	Requests for support or advice, booking training, submitting information	Public task, Legitimate interest	Held by Clerk, contained in e-mails copied to Councillors	Paper copies secured. Electronic copies require password to access.	No longer than ten years unless archived	Yes	Write and Implement policy
Councillor personal information	Names and contact details, declarations of interest, D.O.B.	Recording details of councillors	Legal obligation	Held by Clerk, contained in e-mails copied to Councillors	Paper copies secured. Electronic copies require password to access.	Until no longer a Councillor	Yes	Write and Implement policy

Notes
1. For definitions and usage see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/
2. See PPC GDPR Policy for further detail
3. See PPC GDPR Policy for further detail
4. Privacy notice based on DALC template covers wide range of data collection and use

Reviewed September 2018

Steps for dealing with Subject Access Request under GDPR

What is a Subject Access Request?

An individual is entitled to exercise their rights to obtain information that is held about them under the General Data Protection Regulation 2016. This process is known as a subject access request (SAR). It is generally used by individuals to verify the information that an organisation holds on them – to check that it is accurate, to understand what it is used for and who it might be shared with and occasionally as a pre-cursor to legal action.

Identifying a SAR

Any written enquiry that asks for information we hold about the person making the request can be considered as a SAR, but in many cases there will be no need to treat it as such:

- Can it be dealt with in the normal course of business? If so then do so promptly
- If however you believe it to be a SAR then deal with as per the steps below, remember to log it so that progress can be tracked – details should include the date of receipt, identity of the data subject, summary of the request, indication of whether the PC/Council can comply, date information is sent to the data subject:

Dealing with a SAR

- Verify whether we are controller of the data subject's personal data. If we're merely the processor, inform the data subject and refer them to the actual controller.
- Verify the identity of the data subject; if needed, request any further evidence on their identity. A driving licence, passport or utility bill will be OK – do not retain copies on computer, or in paper files. Just note on the record that you have seen the document and what the document was.
    - Occasionally a request will be made by an individual on behalf of someone else, maybe someone who has power of attorney or a solicitor or another individual who has been appointed by the data subject. Ensure that you have verified it's OK to send the data to the nominated individual – is there a letter of authorisation?
- Verify the request - is it clear what is being asked for? If not, request additional information to help identify any information that meets the request. There is a form on our website for this purpose, and whilst the person making the request is not obliged to fill it in, it will help everyone if they do. The form is available at input web link to form.
- Verify whether the request is unfounded or excessive (in particular because of its repetitive nature); if so, we may refuse to act on the request or could charge a reasonable fee.
- Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in processing it. We are not allowed to charge a fee under GDPR, but there are some types of records that attract a charge.
- Verify whether we process the data requested. If not, inform the data subject accordingly. At all times make sure the record is updated so that progress can be monitored.
- Do not change any data that meets the request once it's been received (such as deletion of anything that might be embarrassing) – this is a criminal act and can lead to prosecution. You can still make routine amendments and deletions to the information as part of normal business.

- Verify whether the data requested includes the personal data of third parties. Make sure that this is redacted before the data is sent out. If it's not possible to do this then ensure that the other data subjects have consented to the supply of their data as part of the SAR process

Responding to a SAR

- You must respond within 1 month after receipt of the request
    - if more time is needed because the response is complex, an extension of up to 2 months is permissible, provided this is communicated to the data subject in a timely manner within the first month;
- if you do not act on the request and are refusing on acceptable grounds, inform the data subject on this decision without delay and at the latest within one month of receipt of the request.
- if the request is submitted electronically, any information should preferably be provided by electronic means as well,
- if you do process the individual's personal data, make sure to include as a minimum the following information in your response:
    - the purposes of the processing;
    - the categories of personal data concerned;
    - the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules or EC model clauses;
    - where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
    - the rights of the individual to request rectification or erasure of personal data (known as 'the right to be forgotten') or restriction of processing of the individual's personal data, or the right of the individual to object to such processing;
    - the right to lodge a complaint with the Information Commissioner;
    - if the data has not been collected from the data subject: the source of such data – obtained from another third party, collected from a website for example, unless the data subject already knows this
    - the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- provide a copy of the personal data in permanent format. If the original request was submitted electronically, then the information should be provided in a commonly used electronic format such as .pdf or .csv.
- explain any abbreviations or complex codes that the data subject might not understand.

If you have any questions about subject access requests then please contact your DPO.

Appendix A

Parwich Parish Council

GDPR Policy. APPENDIX 2. Subject Access Request

Replying to a subject access request providing the requested personal data

Appendix B

Release of part of the information where the remainder is covered by an exemption

Appendix C

Replying to a subject access request explaining why you cannot provide any of the requested personal data

Appendix D

Example form describing data

Appendix A

Replying to a subject access request providing the requested personal data

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of [date] making a data subject access request for [subject].

We are pleased to enclose the personal data you requested.

Include details as per

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely”

Appendix B

Release of part of the personal data, when the remainder is covered by an exemption

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of [date] making a data subject access request for [subject]. To answer your request we asked the following areas to search their records for personal data relating to you:

- [List the areas]

I am pleased to enclose [some/most] of the personal data you requested. [If any personal data has been removed] We have removed any obvious duplicate personal data that we noticed as we processed your request, as well as any personal data that is not about you. You will notice that [if there are gaps in the document] parts of the document(s) have been blacked out. [OR if there are fewer documents enclose] I have not enclosed all of the personal data you requested. This is because [explain why it is exempt].

Include 6(a) to (h) above.

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published, or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely”

Appendix C

Replying to a subject access request explaining why you cannot provide any of the requested personal data

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of [date] making a data subject access request for [subject].

I regret that we cannot provide the personal data you requested. This is because [explanation where appropriate].

[Examples include where one of the exemptions under the data protection legislation applies. For example the personal data might include personal data is 'legally privileged' because it is contained within legal advice provided to the council or relevant to on-going or preparation for litigation. Other exemptions include where the personal data identifies another living individual or relates to negotiations with the data subject. Your data protection officer will be able to advise if a relevant exemption applies and if the council is going to rely on the exemption to withhold or redact the data disclosed to the individual, then in this section of the letter the council should set out the reason why some of the data has been excluded.]

Yours sincerely"

Appendix D

Example form describing data

How to make a request for your information

Under the General Data Protection Regulation you are entitled to ask for access to personal information that we may hold about you. This form will assist you in making a request for your information. It is not compulsory to complete the form but if you do it will help us to locate the information much more quickly. The information that you provide on this form will be treated in confidence.

SECTION 1 PROOF OF IDENTIFICATION

We cannot release information without the right authority to do so. This means that your identity and authority as the person making the request must be verified.

1a. Are you the data subject (the person whom the information is about)? Please tick.

Yes ☐ No ☐

If no, please go to 1b

Please provide **original** proof of identity bearing your name **i.e. driving licence, passport, birth certificate (or certified copy), or an official letter such as from a utility company**. These will be returned to you by recorded delivery. Please tick to state which proof of identity you are enclosing.

1. Birth certificate, passport or driving licence,

2 official letters such as utility bill ☐ ☐

1b Are you acting on behalf of the data subject with their written or other legal authority?

Yes ☐ No ☐

If yes, please state your relationship with the data subject **i.e. parent, legal guardian/carer, solicitor**

Please provide proof that you are legally authorised to do this **i.e. letter of authority or official forms addressed to you on behalf of the data subject**. These will be returned to you by recorded delivery. We reserve the right to request further proof of authority if required.

Please state below what form of proof of authority you have enclosed.

GENERAL DATA PROTECTION REGULATION SUBJECT ACCESS REQUEST FORM SECTION 2 DETAILS OF THE DATA SUBJECT

2a. Details of the Data Subject

Surname:

Forename(s):

Any Previous or Alternative Name(s):

Current Address:

House/Flat number & Street:

Town/City:

County:

Post Code:

Telephone Number:

Please provide details of any previous addresses which you feel may be of assistance to this request.

If you are the data subject, please go to Section 3.

2b. If you making the request on behalf of the data subject, the details will be sent to you with a copy to the data subject (unless you ask for us not to do this). In order for us to send the information to you please complete the details below:

Surname:

Forename:

Name of solicitor(s) (if applicable):

House/Flat number and Street:

Town/City:

County:

Post Code:

Telephone Number:

SECTION 3 DETAILS OF SERVICES

To help us locate the information you are requesting, please complete the appropriate section(s) :

Example of areas where the information might be found:

General Correspondence/Financial transactions/Records such as allotments

Start and end dates of information

Contacts with the organisation

Please send your completed form,
Name/Address

Example Data Breach Assessment Checklist

a) What is the nature of the breach? Please provide as much detail as possible, including what happened, for example loss of laptop containing personal data, email containing personal data sent to wrong recipient

b) How did the breach occur?

c) What type of data is involved, for example, mobile number, medical records etc.?

d) How many individuals are affected?

e) Who are the individuals, for example, employees, customers etc.?

f) What has happened to the data?

g**) Establish a timeline**

a. When did the breach occur?

b. When was it discovered?

c. When was it contained?

h) Was there any protection in place, for example, the data was encrypted, file was password protected?

i) What are the potential consequences for us?

a. Level of severity?

b. How likely are they to occur?

j) **What could the data tell a third party about an individual?**

a. What harm could this cause, for example financial loss, emotional damage etc.?

k) **Does the information have a commercial value that could be exploited, perhaps as part of a criminal activity?**