Farthingstone Parish Council

General Data Protection Regulations (GDPR) May 2018

Portfolio of Policies and Procedures:

Data Protection Policy

Data Breach Policy

Records Retention Policy (updated 16/07/18)

Subject Access Request Procedure

Approved by Farthingstone Parish Council 21st May 2018

For Review May 2019

Data Protection Policy

The Data Protection Policy

Farthingstone Parish Council recognises its responsibility to comply with the General Data Protection Regulations (GDPR) 2018 which regulates the use of personal data. This does not have to be sensitive data; it can be as little as a name and address.

General Data Protection Regulations (GDPR)

The GDPR sets out high standards for the handling of personal information and protecting individuals' rights for privacy. It also regulates how personal information can be collected, handled and used. The GDPR applies to anyone holding personal information about people, electronically or on paper. Farthingstone Parish Council has also notified the Information Commissioner that it holds personal data about individuals.

When dealing with personal data, Farthingstone Parish Council staff and members must ensure that:

Data is processed fairly, lawfully and in a transparent manner

This means that personal information should only be collected from individuals if staff have been open and honest about why they want the personal information.

- **Data is processed for specified purposes only**
  This means that data is collected for specific, explicit and legitimate purposes only.

- **Data is relevant to what it is needed for**
  Data will be monitored so that too much or too little is not kept; only data that is needed should be held.

- **Data is accurate and kept up to date and is not kept longer than it is needed**
  Personal data should be accurate, if it is not it should be corrected. Data no longer needed will be shredded or securely disposed of.

- **Data is processed in accordance with the rights of individuals**
  Individuals must be informed, upon request, of all the personal information held about them.

- **Data is kept securely**
  There should be protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Storing and accessing data

Farthingstone Parish Council recognises its responsibility to be open with people when taking personal details from them. This means that staff must be honest about why they want a particular piece of personal information.

Farthingstone Parish Council may hold personal information about individuals such as their names, addresses, email addresses and telephone numbers. These will be securely kept at the Farthingstone Parish Council Office and are not available for public access. All data stored on the Farthingstone Parish Council Office computers are password protected. Once data is not

needed any more, is out of date or has served its use and falls outside the minimum retention time of Councils document retention policy, it will be shredded or securely deleted from the computer.

Farthingstone Parish Council is aware that people have the right to access any personal information that is held about them. Subject Access Requests (SARs) must be submitted in writing (this can be done in hard copy, email or social media). If a person requests to see any data that is being held about them, the SAR response must detail:

- How and to what purpose personal data is processed
- The period Farthingstone Parish Council tend to process it for
- Anyone who has access to the personal data

The response must be sent within 30 days and should be free of charge.

If a SAR includes personal data of other individuals, Farthingstone Parish Council must not disclose the personal information of the other individual. That individual's personal information may either be redacted, or the individual may be contacted to give permission for their information to be shared with the Subject.

Individuals have the right to have their data rectified if it is incorrect, the right to request erasure of the data, the right to request restriction of processing of the data and the right to object to data processing, although rules do apply to those requests.

Please see "Subject Access Request Procedure" for more details.

Confidentiality

Farthingstone Parish Council members and staff must be aware that when complaints or queries are made, they must remain confidential unless the subject gives permission otherwise. When handling personal data, this must also remain confidential.

Version number	Purpose/change	Author	Date
0.1	Policy	LSS/SH	21/05/18

Date of Review: May 2019

Data Breach Policy

GDPR defines a personal data breach as “a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”. Examples include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

Farthingstone Parish Council takes the security of personal data seriously, computers are password protected and hard copy files are kept in locked cabinets.

Consequences of a personal data breach

A breach of personal data may result in a loss of control of personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data, damage to property or social disadvantage. Therefore, a breach, depending on the circumstances of the breach, can have a range of effects on individuals.

Farthingstone Parish Council’s duty to report a breach

If the data breach is likely to result in a risk to the rights and freedoms of the individual, the breach must be reported to the individual and ICO without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. The Data Protection Officer must be informed immediately so they are able to report the breach to the ICO in the 72 hour timeframe.

If the ICO is not informed within 72 hours, Farthingstone Parish Council via the DPO must give reasons for the delay when they report the breach.

When notifying the ICO of a breach, Farthingstone Parish Council must:

i. Describe the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
ii. Communicate the name and contact details of the DPO
iii. Describe the likely consequences of the breach
iv. Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse effects.

When notifying the individual affected by the breach, Farthingstone Parish Council must provide the individual with (ii)-(iv) above.

Farthingstone Parish Council would not need to communicate with an individual if the following applies:

- It has implemented appropriate technical and organisational measures (ie encryption) so those measures have rendered the personal data unintelligible to any person not authorised to access it;
- It has taken subsequent measures to ensure that the high risk to rights and freedoms of individuals is no longer likely to materialise, or
- It would involve a disproportionate effort

However, the ICO must still be informed even if the above measures are in place.

Data processors duty to inform Farthingstone Parish Council

If a data processor (i.e. payroll provider) becomes aware of a personal data breach, it must notify Farthingstone Parish Council without undue delay. It is then Farthingstone Parish Council's responsibility to inform the ICO, it is not the data processors responsibility to notify the ICO.

Records of data breaches

All data breaches must be recorded whether or not they are reported to individuals. This record will help to identify system failures and should be used as a way to improve the security of personal data.

Record of Data Breaches

Date of breach	Type of breach	Number of individuals affected	Date reported to ICO/individual	Actions to prevent breach recurring

To report a data breach, use the ICO online system:

https://ico.org.uk/for-organisations/report-a-breach/

Version number	Purpose/change	Author	Date
0.1	Policy	LSS/SH	21/05/18

Next review date: May 2019

Records Retention Policy

Farthingstone Parish Council recognises that the efficient management of its records is necessary to comply with its legal and regulatory obligations and to contribute to the effective overall management of the association. This document provides the policy framework through which this effective management can be achieved and audited.

It covers:

- Scope
- Responsibilities
- Retention Schedule

Scope

This policy applies to all records created, received or maintained by Farthingstone Parish Council in the course of carrying out its functions. Records are defined as all those documents which facilitate the business carried out by Farthingstone Parish Council and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically. A small percentage of Farthingstone Parish Council records may be selected for permanent preservation as part of the Councils archives and for historical research.

Responsibilities

Farthingstone Parish Council has a corporate responsibility to maintain its records and record management systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Clerk. The person responsible for records management will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and timely. Individual staff and employees must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with Farthingstone Parish Council's records management guidelines.

Retention Schedule

The retention schedule refers to record series regardless of the media in which they are stored.

Document	Minimum Retention Period	Reason
Minutes		
Minutes of Council meetings	Indefinite	Archive
Minutes of committee meetings	Indefinite	Archive
Employment		

Staff employment contracts	6 years after ceasing employment	Management
Staff payroll information	3 years	Management
Staff references	6 years after ceasing employment	Management
Application forms (interviewed – unsuccessful)	6 months	Management
Application forms (interviewed – successful)	6 years after ceasing employment	Management
Disciplinary files	6 years after ceasing employment	Management
Staff appraisals	6 years after ceasing employment	Management
Finance		
Scales of fees and charges	6 years	Management
Receipt and payment accounts	Indefinite	VAT
Bank statements	Last completed audit year	Audit
Cheque book stubs	Last completed audit year	Audit
Paid invoices	6 years	VAT
Paid cheques	6 years	Limitation Act 1980
Payroll records	6 years plus current year	HMRC
Petty cash accounts	6 years	Audit
Insurance		
Insurance policies	6 years after policy end	Management
Certificates for Insurance against liability for employees	6 years after policy end	Management
Certificates for Public Liability	6 years after policy end	Management
Insurance claim records	6 years after policy end	Management
Health and Safety		
Accident books	3 years from date of last entry	Statutory
Risk assessment	3 years	Management
General Management		
Councillors contact details	Duration of membership	Management
Lease agreements	12 years	Limitation Act 1980
Contracts	6 years	Limitation Act 1980
Email messages	At end of useful life	Management
Consent forms	5 years	Management
GDPR Security Compliance form	Duration of membership	Management

Version number	Purpose/change	Author	Date
0.1	Initial draft	LSS	20/2/18
0.2	Amend retention times	LSS/SH	17/15/18 Approved 16/07/18

Next review date: May 2019

Subject Access Request Procedure

This procedure is to be followed when an individual contacts Farthingstone Parish Council to request access to their personal information held by the Council. Requests must be completed within 1 month, so it should be actioned as soon as it is received. SAR's should be provided free of charge; however, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The steps below should be followed to action the request:

1. Is it a valid subject access request?
    a) The request must be in writing (letter, email, social media or fax).
    b) Has the person requesting the information provided you with sufficient information to allow you to search for the information? (You are allowed to request for more information from the person if the request is too broad.)

2. Verify the identity of the requestor.
    a) You must be confident that the person requesting the information is indeed the person the information relates to. You should ask for the person to attend the office with their passport/photo driving licence and confirmation of their address (utility bill/bank statement).

3. Determine where the personal information will be found
    a) Consider the type of information requested and use the data processing map to determine where the records are stored. (Personal data is data which relates to a living individual who can be identified from the data (name, address, email address, database information) and can include expressions of opinion about the individual.)
    b) If you do not hold any personal data, inform the requestor. If you do hold personal data, continue to the next step.

4. Screen the information
    a) Some of the information you have retrieved may not be disclosable due to exemptions, however legal advice should be sought before applying exemptions. Examples of exemptions are:
        - References you have given
        - Publicly available information
        - Crime and taxation
        - Management information (restructuring/redundancies)
        - Negotiations with the requestor
        - Regulatory activities (planning enforcement, noise nuisance)

- Legal advice and proceedings
- Personal data of third parties

5. Are you able to disclose all the information?
    a) In some cases, emails and documents may contain the personal information of other individuals who have not given their consent to share their personal information with others. If this is the case, the other individual's personal data must be redacted before the SAR is sent out.

6. Prepare the SAR response (using the sample letters at the end of this document) and make sure to include as a minimum the following information:
    a) the purposes of the processing;
    b) the categories of personal data concerned;
    c) 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;
    d) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
    e) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
    f) the right to lodge a complaint with the Information Commissioners Office ("ICO");
    g) if the data has not been collected from the data subject: the source of such data;
    h) 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.

    Be sure to also provide a copy of the personal data undergoing processing.

All SAR's should be logged to include the date of receipt, identity of the data subject, summary of the request, indication of if the Council can comply, date information is sent to the data subject.

Sample letters:
Replying to a subject access request providing the requested personal data

"[Name] [Address]

[Date]

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 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"

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

"[Name] [Address]

[Date]

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"

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

"[Name] [Address]

[Date]

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"

Version number	Purpose/change	Author	Date
0.1	Procedure	LSS/SH	20/05/18

Next review date: May 2019