

PART I –
DATA PROTECTION POLICY
(adopted 29 May 2018, revised 29 January 2019)

This policy is drawn up in accordance with the requirements of the Data Protection Act 1998 (DPA), as supplemented by the General Data Protection Regulations (GDPR) which came in to force on 25 May 2018. It relates to personal data held by the Parish Council about living identifiable individuals.

Preamble.

The Parish Council adopted a Data Protection policy based on the requirements of the DPA in 2015. The GDPR is based on the DPA and expands the legal requirements of Parish Council. The GDPR requires organisations to create three posts:

Data Protection Officer (DPO). Parish Councils are **exempt** from this requirement.

Data Controller (DC). The person / organisation who determines how and what data is processed. This is the Parish Council as a corporate body.

Data processor (DP). The person / organisation which processes the data. This is the Clerk.

The Data Controller must maintain a record of processing activities for which it is responsible.

The Data Processor must maintain a record of processing activities carried out for the Data Controller.

Privacy Notices must be sent and acknowledged to all Council members and others whose data is held. There are two types of privacy Notice (one for the public and one for Council members and staff) which are available to view on the Parish Council web site.

The Parish Council must be able to produce evidence of consent to hold and process all personal data.

Prior to 25 May 2018 all staff and members of the Parish Council were contacted with a copy of the Privacy Notice and requested to acknowledge receipt of it.

Prior to 25 May 2018 all members of the public whose personal details were held were contacted with a request to positively opt-in to receiving information from the Parish Council; they were also sent Privacy Notice. Failure to opt-in will result on that persons' data being removed from the Parish Council records.

The revised Data Protection Policy, effective from 25 May 2018 is:

Policy 1. Information we hold

The only information we hold comprises name and email address. We may also hold mailing name and telephone number. All information held has been obtained from the data subject or is publicly available elsewhere (eg telephone directory, but NOT the Electoral Register).

We hold no other personal information – eg 'sensitive personal data' – about the data subject. 'Sensitive Personal Data' is information about racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual orientation or genetic or biometric data.

Policy 2. Communicating private information

We do not share personal data with any third party, other than members of Newland Parish Council and those with whom we are obliged, by law, to share it. If disclosure to such a third party requires the data subject's permission it will be obtained before the information is divulged. All 'multi-addressed' emails are sent 'bcc'.

Policy 3. The lawful basis upon which we hold and process personal data.

We hold the data for the sole purpose of communicating information which we consider the recipient will find of interest, such as Parish Council meetings agendas and minutes, news and activities, and for forwarding similar information from third parties.

Policy 4. Retention of personal data

We retain the information as long as it is relevant, or until the data subject requests us to delete it.

Policy 5. The data subjects' rights.

We will comply with the GDPR in respect of the individuals' right:

- 5.1 to be informed of the data we hold
- 5.2 of access to data we hold
- 5.3 to rectification of any erroneous data hold
- 5.4 to erasure of any data we hold
- 5.5 to restrict the processing of any data we hold
- 5.6 to data portability - this only applies to
 - personal data an individual has provided to a controller;
 - where the processing is based on the individual's consent or for the performance of a contract;
 - when processing is carried out by automated means
- 5.7 to object
- 5.8 not to be subject to automated decision making, including profiling

Policy 6. Subject access requests (SARs)

All requests for information will be supplied free of charge, in a clear format and within 1 calendar month. Requests which are considered manifestly unfounded, excessive or vexatious will be refused. Any request refused will be accompanied by a clear reason and the advice that the person has a right to complain to the supervisory authority, and to a judicial remedy.

1. Data held by the Parish Council (NPC) is easily accessible to enable swift responses to SARs.

UPON RECEIPT OF A SAR

2. SARs should be addressed to the Data Controller (NPC)
3. Verify the identity of the data subject (the originator of the SAR)
4. Clarify, if necessary, what data is requested.
5. Acknowledge receipt of the SAR.
6. Verify if NPC holds the data requested
7. NPC to ensure data is not altered as a result of the SAR

8. If the data requested contains data on other data subjects, filter this data out of the response.

RESPONDING TO A SAR

9. Respond as soon as possible, but certainly within 1 month. For complex requests a further 2 months will be permitted if advised to the enquirer within the first month.
10. If NPC is unable to supply the data requested, the enquirer will be informed within 1 month.
11. If the SAR is requested electronically then the reply will also be by electronic means.
12. The enquirer will be advised, as part of the response
 - a. if data on the data subject is processed, the purposes of the processing;
 - b. the category of personal data concerned;
 - c. details of recipients with whom personal data had been disclosed
 - d. where possible, the envisaged period for which personal data will be stored
 - e. the existence of the right to request rectification or erasure of personal data, or restriction of processing of personal data, or to object to such processing.
 - f. The right to lodge a complaint with the ICO
 - g. Where the data has been obtained, if not from the data subject
13. Provide a copy of the personal data undergoing processing.

Policy 7. Consent

Consent to the processing of personal data will be obtained by a specific opt-in request by the data subject. A record of all such consents held will be maintained by the Data Processor.

Policy 8. Children

We will process no data for a child without consent from a person holding 'parental responsibility'.

Policy 9. Data breaches.

We have procedures in place to effectively detect, report and investigate a personal data breach.

In the case of a data breach which is likely to result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage, we will notify the Information Commissioners Office (ICO).

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we will, additionally, notify those concerned directly.

Policy 10. Data Protection Impact Assessments (DPIAs)

We will undertake a DPIA where data processing is likely to result in a high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data

If a DPIA indicates that the data processing is high risk we will seek guidance from the ICO.

Policy 11. Internal audit

Two Councillors appointed by the Parish Council (the Data Controller) will, annually, undertake an internal audit of GDPR procedures and recommend alterations where appropriate. The audit outcome will be confirmed by full Council at the time of the routine review of this policy.