Scarning Parish Council

General Data Protection Regulation Policy

POLICY STATEMENT

Scarning Parish Council recognises its responsibility to comply with General Data Protection Regulations.

IMPLEMENTATION

This policy updates the Parish Council's Data Protection Policy (adopted on 8 May 2017) and procedures to include the additional requirements of GDPR which will apply in the UK from May 2018. The Government has confirmed that despite the UK leaving the EU, GDPR will still be a legal requirement. This policy explains the duties and responsibilities of the Council and identifies the means by which the Parish Council will meet its obligations.

IDENTIFYING THE ROLES AND MINIMISING RISK

GDPR requires that everyone within the Parish Council must understand the implications of GDPR and that roles and duties must be assigned. The Parish Council is the Data Controller and the Clerk is the Data Protection Officer (DPO).

Personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; be adequate, relevant and limited to what is necessary for processing; be accurate and kept up to date; be kept only for as long as is necessary for processing; and be processed in a manner that ensures its security.

The handling of information is seen as a high/medium risk to the Council (both financially and in terms of its reputation) and one which must be included in the Council's Risk Management Policy. Such risk can be minimised by undertaking an Information Audit; issuing privacy statements; maintaining privacy impact assessments (an audit of potential data protection risks with new projects); minimising who holds data protected information; ensuring the safe disposal of information; and the Parish Council undertaking training in data protection awareness.

GDPR requires continued care by the Clerk and councillors in the sharing of information about individuals, whether as a hard copy or electronically. A breach of the regulations could result in the Parish Council facing a fine from the Information Commissioner's Office (ICO) for the breach itself and also to compensate the individual(s) who could be adversely affected.

INFORMATION AUDIT

The Data Protection Officer must undertake an Information Audit which details the personal data held, where it came from, the purpose for holding that information and

with whom the Parish Council will share that information. This will include information held electronically or as a hard copy. Information held could change from year to year with different activities, and so the Information Audit will be reviewed at least annually or when the Parish Council undertakes a new activity. The Information Audit review should be conducted ahead of the review of this policy and the reviews minuted.

PRIVACY NOTICES

Being transparent and providing accessible information to individuals about how the Parish Council uses personal data is a key element of the Data Protection Act 1998 and the General Data Protection Regulations (GDPR). The most common way to provide this information is in a privacy notice. This is a notice to inform individuals about what the Council does with their personal information. A privacy notice will contain the name and contact details of the Data Controller and Data Protection Officer; the purpose for which the information is to be used; and the length of time for its use. It should be written clearly and should advise the individual that they can, at any time, withdraw their agreement for the use of this information. Issuing of a privacy notice must be detailed on the Information Audit kept by the Parish Council. The Parish Council will adopt a privacy notice to use, although some changes could be needed depending on the situation, for example where children are involved.

CHILDREN

There is special protection for the personal data of a child. The age when a child can give their own consent is 13. If the Parish Council requires consent from young people under 13, the Council must obtain a parent or guardian's consent in order to process the personal data lawfully. Consent forms for children age 13 plus, must be written in language that they will understand.

INDIVIDUALS' RIGHTS

GDPR gives individuals rights with some enhancements to those rights already in place:

- the right to be informed.
- the right of access.
- the right of rectification.
- the right to erasure.
- the right to restrict processing.
- the right to data portability.
- the right to object.

- the right not to be subject to automated decision-making, including profiling.

The two enhancements of GDPR are that individuals now have a right to have their personal data erased (sometime known as the 'right to be forgotten') where their personal data is no longer necessary in relation to the purpose for which it was originally collected and data portability must be done free of charge. Data portability refers to the ability to move, copy or transfer data easily between different computers.

If a request is received to delete information, then the DPO must respond to this request within a month. The DPO has the delegated authority from the Parish Council to delete information.

If a request is considered to be manifestly unfounded then the request can be refused .

Any charges applicable will be detailed in the Council's Freedom of Information Publication Scheme.

DATA BREACHES

One of the duties assigned to the DPO is the investigation of any breaches. Personal data breaches should be reported to the DPO for investigation. The DPO will conduct this with the support of the Personnel Committee. Investigations must be undertaken within one month of the report of a breach. The ICO will be advised of a breach (within 3 days) where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will also have to notify those concerned directly.

It is unacceptable for non-authorised users to access IT using employees' log-in passwords or to use equipment while logged on. It is unacceptable for employees, volunteers and members to use IT in any way that may cause problems for the Parish Council, for example the discussion of internal Council matters on social media sites could result in damage to the Parish Council's reputation and to individuals.

ACTION TO BE TAKEN

The main actions arising from this policy are:

- A copy of this policy will be made available on the Parish Council's website. The policy will be considered as a core policy of the Council.

- Privacy notices must be issued.

- Data Protection will be included in the Parish Council's Risk Management Policy.

- The Clerk's contract and Job Description will be amended to include additional responsibilities relating to Data Protection.

- An Information Audit will be conducted and reviewed at least annually, or when projects and services change.

POLICY REVIEW

This policy will be reviewed at least annually or when further advice is issued by the ICO.

All employees, volunteers and councillors are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of the Parish Council.

Agreed: January 2019

Review Date: January 2020

General Data Protection Regulation

What is GDPR?

GDPR replaces the Data Protection Act of 1998. It is a Regulation which affects all authorities which collect personal data. The Parish Council collects and uses personal data for a number of reasons. I, as clerk and all councillors are expected to understand the implications of GDPR. It is ultimately the responsibility of the Parish Council, as the Data Controller, to ensure that things are done correctly.

There is an obligation on all members of the Parish Council to be trained in this matter. Understanding the implications of this Regulation is one of the best ways of avoiding breaches in respect of personal data which could be costly for the Council, as well as a risk to the Council's reputation.

Compliance

Although GDPR does not come into force until May 2018, we are being encouraged by the Information Commissioner's Office to put into place all the things which the Regulation will expect us to do ahead of this date. GDPR is an EU law which the UK Government has confirmed will apply to this country. The Government will be passing its own legislation on the matter next year.

Things to be done – recognising the roles

The Parish Council, as Data Controller, must appoint a Data Protection Officer (DPO). This will need to be someone who is familiar with the workings of the Council as well as GDPR and with no conflict of interest in determining the purpose or manner of processing personal information. The DPO could be the Clerk. If it is the Clerk this will need to be included in my Job Description and Contract of Employment. We will also need to amend our Standing Orders at their next review (certainly before May 2018) to include an Order which recognises the Parish Council as the Data Controller and the appointment of a DPO. The Order should also say that all councillors should be trained in GDPR.

Additional work for the DPO

The DPO will need to prepare an Information Audit of personal information held. This audit must detail not only the information held, but the reason for it being held along with other information. The DPO must also issue Privacy Notices to people whose personal information is held by the Council. The DPO will need to include GDPR in the Parish Council's Risk Management Schedule and undertake assessments of projects which might pose considerable risk in respect of data protection. I have drafted a GDPR Policy for adoption, below.