General Data Protection Regulation (GDPR)

What is GDPR?

GDPR is EU legislation that will come into force on 25th May and will replace the Data Protection Act of 1998. It is a Regulation which affects all organisations including local authorities which collect personal data. We collect and use personal data for a number of reasons in order to carry out the work of the council. It is ultimately the responsibility of the Council, as the Data Controller, to ensure that things are done correctly.

The GDPR requires that data shall be:

(taken from Article 5 of the GDPR)

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition "the controller (Parish Council) shall be responsible for, and be able to demonstrate, compliance with the principles."

What needs to be done?

1. **Appoint a Data Protection Officer (DPO)**
   The Data Controller (the Council) 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. I suggest you appoint me, as Clerk, as the DPO.

2. **Establish a Data Protection Committee**
   If I, as Clerk, am to be appointed the DPO we will need to be careful that it is the Council determines the purpose or manner of processing personal information. To satisfy this requirement I suggest that we establish a Data Protection

Committee (suggested Terms of Reference are included – appendix A). This committee should meet prior to the 25th May and again at least annually.

3. **Amend the Clerk's Job Description and Contract**
   It will be necessary to amend my Job Description and Contact. Suggested amended wordings are included – appendix B.

4. **Amend Standing Orders**
   It is important we all understand our responsibilities with regard to Data Protection. We will need to amend our Standing Orders to include an Order which recognises the Council as the Data Controller and states who the DPO is. The Order should also detail the responsibilities of councillors and me as Clerk. Suggested insertion for Standing Orders are included – appendix C.

5. **Data Protection Policy**
   We need a Data Protection Policy which lays out how the Council manages data and the responsibilities. A suggested policy is included – appendix D. This policy along with a statement regarding Data Protection (included – appendix E) will need to be published on the Council's website.

Additional work for the DPO/Clerk

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 Council's Risk Management Schedule and undertake assessments of projects which might pose considerable risk in respect of data protection.

Julie King
March 2018

Appendix A

Data Protection Committee
Terms of Reference

Meetings

The Committee will meet at least once a year. Meetings are open to the public. An agenda is prepared for each meeting and minutes written from each meeting. Minutes are presented to the next full council meeting by the Chairman of the Committee for adoption by the Council.

Membership

The Committee will be made up of three councillors. The Committee will be appointed at the Annual Parish Council meeting. A Chairman of the Committee for the year, will be elected at the first committee meeting following the Annual Parish / Town Council Meeting.

Aims and Objectives of the Committee

The Committee aims:

- To determine the purpose and manner of processing personal data according to the law
- To ensure that the Clerk as Data Protection Officer (DPO) has no conflict of interest with this process
- To ensure that councillors and staff receive ongoing and appropriate training for Data Protection
- To conduct a survey of the Information Audit, Privacy Notices and any Risk Management to ensure compliance with Data Protection
- To receive any reports from the DPO of any manifestly unfounded requests and confirm action to be taken
- To receive reports from the DPO of any investigation of breaches which might need to be undertaken
- To make an annual review of the GDPR Policy and recommend any changes to Council which might be required
- To recommend to Council any changes which may be required in Standing Orders in respect of Data Protection
- To recommend to Council any changes which may be required to the Job Description and Contract of Employment for the Clerk / DPO.

Budget

The Committee does not have its own budget but will recommend any budgetary needs to the Council in respect of the administrative and staffing costs to implement and maintain Data Protection requirements.

Appendix B

Contract of Employment amendment for Data Protection

(insert number in Contract) DATA PROTECTION

The Parish Clerk is the Data Protection Officer (DPO) and Data Processor for the Council. The Council and all of its employees must comply with data protection laws. You have a duty to ensure that the Council and its employees understand about data protection and can comply with its obligations. To support you with this duty, you will be given training on data protection.

Job Description addition for Data Protection

- To be the Data Protection Officer for the Council, maintaining independence from the processes involved.

Appendix C

Insertion in Standing Orders for Data Protection

(Insert number of the order) Data Protection

a) The Council is the Data Controller and the Parish Clerk is the Data Protection Officer.

b) Councillors and staff must understand their obligations regarding Data Protection and where necessary receive training.

c) Data Protection is managed through a Committee and a Policy.

Appendix D

Data Protection Policy

Purpose of the policy and background to the General Data Protection Regulation

This policy explains to councillors, staff and the public about GDPR. 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. This policy updates any previous data protection policy and procedures to include the additional requirements of GDPR which apply in the UK from May 2018. The Government have 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 it identifies the means by which the council will meet its obligations.

Identifying the roles and minimising risk

GDPR requires that everyone within the council must understand the implications of GDPR and that roles and duties must be assigned. The Council is the data controller and the clerk is the Data Protection Officer (DPO) and the data processor. It is the DPO's duty to undertake an information audit and to manage the information collected by the council, the issuing of privacy statements, dealing with requests and complaints raised and also the safe disposal of information. This is included in the Job Description of the clerk.

Appointing the Clerk as the DPO must avoid a conflict of interests, in that the DPO should not determine the purposes or manner of processing personal data.
GDPR requires continued care by everyone within the council, councillors and staff, in the sharing of information about individuals, whether as a hard copy or electronically. A breach of the regulations could result in the 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. Therefore, the handling of information is seen as high / medium risk to the council (both financially and reputationally) and one which must be included in the Risk Management Policy of the council. 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 and the council undertaking training in data protection awareness.

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 Data Protection Committee. Investigations must be undertaken within one month of the report of a breach. Procedures are in place to detect, report and investigate a personal data 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 Council, for example the discussion of internal council matters on social media sites could result in reputational damage for the Council and to individuals.

Privacy Notices
Being transparent and providing accessible information to individuals about how the Council uses personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice. This is a notice to inform individuals about what a 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 (if applicable). Issuing of a privacy notice must be detailed on the Information Audit kept by the council. The council will adopt a privacy notice to use, although some changes could be needed depending on the situation, for example where children are involved. Where consent is being relied on as the lawful basis for processing the data, privacy notices must be verifiable.

Information Audit
The DPO 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 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 council undertakes a new activity. The information audit review should be conducted ahead of the review of this policy and the reviews should be minuted.

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 to rectification
- the right to erasure
- the right to restrict processing
- 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 Council to delete information.

If a request is considered to be manifestly unfounded then the request could be refused or a charge may apply. The Data Protection Committee will be informed of such requests and will determine the charge.

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 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.

Summary
The main actions arising from this policy are:

- The Council must be registered with the ICO.
- A copy of this policy will be available on the Council's website. The policy will be considered as a core policy for the Council.
- The Clerk's Contract and Job Description (if appointed as DPO) includes additional responsibilities relating to data protection.
- An information audit will be conducted and reviewed at least annually or when projects and services change.
- Privacy notices must be issued.
- Data Protection is included on the Council's Risk Management Policy.
- A Committee, with Terms of Reference, manages the process.

This policy document is written with current information and advice. It 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 Council.

This Policy is supported by the Terms of Reference for the Data Protection Committee (attached).

Appendix E

Data Protection Commitment – for website

Our Data Protection commitment

We are committed to managing your data securely and responsibly. Please refer to our Data Protection Policy, which details how we manage the processes required under the General Data Protection Regulations and the Data Protection Act.

Your marketing preferences

If we produce marketing material, in hard copy or electronically, and you have indicated that you would like to receive it, we will do this through a Consent Form (Article 6 (a) – GDPR). This means we will only use your data to send you the information you have chosen to receive. If your preferences change you can unsubscribe from our mailings at any time. If we want to use your personal data for anything else we will let you know and ask you to complete a Consent Form.

Your data and third parties

We may use selected third parties to help deliver services to, and to support our council commitments to you or your organisation. Sometimes we are legally required to give information to certain authorised agencies but we will not share your data with any third parties for marketing or other purposes, unless you have told us that you are happy for us to do this.

Your rights

You have some important rights that determine how and whether we use your data. As an example, you can just as easily decide not to receive our mailings as doing so.

Your privacy is extremely important to us so, if you think we are not handling your data properly we want you to tell us. And after that, if you feel that we are not getting it right, you can complain to the Information Commissioner www.ico.org.uk

Privacy Statement

Our Privacy Statements contain the contact details of our organisation and explains who is who within it. They advise the legal right under Data Protection (Article 6 (c) and (e) - GDPR) which entitle us to hold and use personal data. At the same time, they explains why we need to hold or process personal data. The Privacy Statements also explain data subject rights in respect of Data Protection. If you have been issued with a privacy statement, please take a moment to read it.