DRAFT REPORT TO COUNCIL

1. INTRODUCTION

1.1 This report updates Council on the new General Data Protection Regulation (GDPR) which will replace the longstanding Data Protection Act (1998). GDPR will come into force on 25th May 2018. It significantly tightens up the rules on privacy and consent and the implications for councils are widespread. Local Councils and Parish Meetings must comply and put in suitable arrangements for the control of personal data held and processed by the Council (the Data Controller).

1.2 The concepts and principles of GDPR are broadly similar with the 1998 in that personal data must be:

- Must be processed lawfully, fairly and transparently;
- Is only used for a specific processing purpose that the data subject has been made aware of and no other, without further consent;
- Should be adequate, relevant and limited i.e. only the minimum amount of data should be kept for specific processing;
- Must be accurate and where necessary kept up to date;
- Should not be stored for longer than is necessary, and that storage is safe and secure.

1.3 However, Councils will have to do some things for the first time and be more proactive on the way they manage data. Changes include new reporting requirements, increased fines and penalties, new rules on obtaining consent and writing privacy notices. Other changes to note include:

- Councillors and staff must have suitable training;
- It is not mandatory for town and parish councils to appoint a Data Protection Officer but it is considered good practice;
- The £10 charge for a data subject access request has been removed;
- Council must respond to a Subject Access Request (SAR) in a calendar month. Previously this was 40 days;
- Councils will no longer be required to register with the Information Commissioner's Office (ICO) but will be required to pay an annual fee of £40 to £60 depending on the number of employees;
- Breaches must be notified to the ICO normally within 72 hours;
- Failure to comply with the new law places significant risk with fines of £17M or 4% of global turnover, whichever is the greater.

1.4 Among the many challenges to implement the changes as effectively and efficiently as possible is the data audit of data collected and identify whether consent was granted correctly, or at all. There will also be a requirement to delete records where consent was not given or where new consent is not provided.

1.5 In future, as part of GDPR, local authorities will also need to ensure that privacy is designed into their processes and services by default.

1.6 In order to achieve compliance with the new Regulations, Council has undertaken a data audit of personal and other data it has collected to establish what data is held, where and how it is stored, the purpose it is collected, whether consent has been granted, any measures in place to ensure data security and who controls it. Data Control may be by the Council itself or via a third party (payroll, pensions etc).

1.7 The data audit should also assess existing organisational processes for data protection and deletion and assess how vulnerable data held and stored may be.

2. CONSENT

2.1 As part of the new Regulations Councils must put into place proactive processes to ensure consent is obtained where required. The Regulations stipulate that individuals must give their explicit and 'informed' consent for their data to be retained. That consent will include the period of time information will be held and processed. This will mean that individual must be made aware of how their information will be used, whether it will be shared and who is responsible.

2.2 In order to comply with this requirement the following actions will be required:

- GDPR states that consent has to be specific, informed, unambiguous and freely given, which means that individuals cannot be chased or unduly pressed for their consent. Therefore, Councils will need to apply much more rigour to this process, because records also need to be kept to evidence that consents have been properly secured;
- Councils will need to consider the position of minors, because children under the age of 13 cannot give consent;
- There are issues with 'sensitive personal data', which includes data revealing racial or ethnic origin, political opinions etc. Councils, like any other organisation, will need explicit and specific consent for the exact purpose or purposes for which any of this sensitive personal data will be used.

2.3 GDPR does not allow Consent for one type of data processing to give councils permission to do anything else with the personal data. Therefore if consent is required from a resident to be added to a newsletter mailing list and their details are used for a different purpose such as promoting the facilities of the Council the Council would need to request consent separately. The two elements can be included on the same form but there would need to be two consent boxes explaining why each consent is required. Where councils collect consents that are to be added to a email mailing list, these consents will need to be recorded. Councils may need several different consent forms (or elements within a single form) to cover different areas of data processing within the activities of the council.

2.4 The ICO has issued draft guidance on consent and recommend that consent should be relied on sparingly. There may be other legal grounds available and

councils should only consider consent as ‘the last resort’ particularly as it can be easily withdrawn.

2.5 For staff, volunteers, and councillors, councils should not rely on consent because under GDPR, and the present law, consent must be freely given. As it is necessary to process certain personal data for these staff, councillors and other role holders to allow them to perform their roles, and the balance of power between them and the council is unequal, consent cannot be said to be ‘freely given’. However, even where there is no requirement to obtain specific consent, these individuals should be sent a “Privacy Notice” explaining why the council is holding their data, what it will do with it, how long it will be kept and how it can be amended/updated

3. PRIVACY NOTICES

3.1 The transparency requirements under the GDPR require councils to provide individuals with extensive information about how their personal data is collected, stored and used. In practice, this means that councils will need to include more information in their privacy policies, as well as retaining more detailed records of their data processing activities in relation to their staff, customers and third parties. This means developing a new, much more user friendly Privacy Policy and Privacy Notices written in plain English.

3.2 The GDPR sets out six lawful bases for processing data. Unless an exemption applies, at least one of these will apply in all cases. It is possible for more than one to apply at the same time. One of the new requirements for Privacy Notices is that councils must set out in the Privacy Notice which Lawful basis they are relying on. For most councils, the relevant ones will be:

- 1 – Consent (but not for staff, councillors and other role holders),
- 2 – Compliance with a legal obligation (which includes performance of statutory obligations),
- 3 – Contractual necessity (for example with contractors)
- 4 – Public interest

4. DATA PROTECTION OFFICER (DPO)

4.1 Town and parish councils will not now be required to appoint a DPO but it will be considered best practice. The DPO may be an internal or external appointment. This means that the DPO may be a staff member or engaged under a service contract. However, anyone who makes decisions regarding the processing data would be deemed to have a conflict of interest and cannot act as a DPO. This is because one cannot undertake due diligence or governance on oneself.

4.2 This will mean that Clerks, Chief Officers and RFOs cannot be designated as a Council’s DPO. There will be a conflict of interest between the role of a clerk and RFO. The DPO must be allowed to perform tasks in an independent manner and should not receive any instructions regarding the exercise of their tasks.

4.3 The council, as data controller, remains responsible for compliance with the data protection legislation including the GDPR. Monitoring of compliance does not mean that it is the DPO who is personally responsible where there is an instance of non-compliance. The GDPR makes it clear that it is the controller, not the DPO, who is required to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.

4.4 A DPO's duties include:

- Informing and advising the council and its staff of their obligations under GDPR and other data protection laws;
- Monitoring compliance of the council, both its practices and policies, under GDPR and other data protection laws;
- Raising awareness of data protection law;
- Identifying relevant training to staff and councillors;
- Organising and carrying out data protection-related audits;
- Providing advice to the council, where requested, in relation to the carrying out of data protection impact assessments ('DPIAs') and the council's wider obligations with regard to DPIAs;
- Acting as a contact point for the Information Commissioner's Office.

5. INCREASED RIGHTS OF INDIVIDUALS

5.1 GDPR stipulates enhanced rights of citizens. These include:

- The right to be forgotten;
- The right to make a Subject Access Request (SAR) at any time;
- The right to have their data protected by processes of encryption or pseudonymisation;
- The right to prevent direct marketing;
- The right to prevent automated decision-making and profiling, and
- The right to obtain and reuse any data held

5.2 The GDPR will give people more rights over their data. This will include individuals being given the right to have personal data deleted. In order to do this Councils will need to be able to find the data and to have someone who is responsible for making sure that happens.

5.3 Individuals also have the right to know what data is held on them, why the data is being processed and whether it will be given to any third party. They have the right to be given this information in a permanent form (hard copy). This is known as a 'subject access request' or "SAR". Councils need to be able to identify a SAR, find all the relevant data and comply within one month of receipt of the request. Under the GDPR the time limit for responding to SARs is reduced from 40 days to one calendar month and the £10 fee is abolished.

5.4 With regard to risks, the GDPR will impose new burdens on councils, including new reporting requirements that will place additional pressures on staff resources. The increase in fines (from £500,000 in the UK to the greater

of £17 million or 4% of global annual turnover) also places significantly additional risk on councils. The GDPR will also allow users to claim damages where there has been a data breach or where processing of data is unlawful.

6. ACTION PLAN

6.1 The table below sets out the initial actions required to be undertaken by Council and the basic documentation that the Council will need to put in place to demonstrate that it is working towards compliance. A more detailed action plan has been provided as part of the data audit undertaken.

Data Audit	The Data Audit has: • Identification of what personal data is held; • How personal data is collected; • Records management; • Information sharing	New Document Retention Policy to be adopted as part of GDPR compliance
Data Processing Log	A log will be provided as part of the Data Audit.	New activities will be included.
Consent Forms	Data audit has identified required consent forms.	Record will be kept of how and when consent is obtained
Privacy Notice and Privacy Policy	Review/update existing Must be transparent and clear in plain language, easy to access. Provided as part of the Data Audit.	Detailed privacy notices to be uploaded onto the website
Data Protection Policy	Adopt revised Policy.	Upload onto website
Date Subject Access Request Policy	Adopt revised policy	Sample response letters have been included

7. RECOMMENDATIONS

7.1 Council is requested to consider the following:

- That Council adopts this report;
- That Council adopts the Data Audit report and the action plan;
- That Council adopts the following policies and procedures:
  - Data Protection Policy
  - Data Retention Schedule
  - Data Privacy Impact Assessment procedure
  - Privacy Notices and Consent forms
  - Data Subject Access Request information and form
  - Data Breach Procedure
- That Council considers the appoint of a Data Protection Officer as good practice and to provide on-going advice to the Clerk and Council.