THE GENERAL DATA PROTECTION REGULATION (GDPR)

1.0 INTRODUCTION

1.1 The General Data Protection Regulation (GDPR) is the biggest change to data protection law in over 20 years. The regulation is EU law and will be coming into force without the need for UK legislation on 25 May 2018. A new Data Protection Bill is also due to be enacted by 25 May 2018 which incorporates the GDPR, this new legislation will increase the powers of the Information Commissioner and the level of fines for non-compliance.

1.2 All local councils will need to comply with the legislation. While the GDPR has many similarities to the Data Protection Act 1998 it brings a 21st century modernising approach to the processing of personal data in the digital age. Imposing new obligations on controllers and for the first-time data processors as well as expanding the rights individuals have over the use of their personal information impacting people, processes and technology across all business functions.

1.3 A major change requires organisations not only to show compliance through the existence of policies, procedures and staff training but to be able to demonstrate how in each case it has complied with GDPR requirements. To protect the data held and to comply with the GDPR in how the data is processed councils should undertake the following key tasks:

- Complete a data audit
- Adopt new policies or review existing policies:
- Privacy Notices
- Document retention and disposal policy
- Appoint a Data Protection Officer
- Adopt a Security Incident Response Policy

1.4 Undertaking a data audit may provide an opportunity to go through council/meeting files and decide which documents need to be kept and which do not. One of the most important aspects of the data audit is to define the lawful basis for processing data. In the data audit it is necessary to:

- Define the personal data
- Say what the purpose of processing is

- Define how the data is processed
- Define the lawful basis for processing
- Specify how the information was acquired
- Define how it is stored and kept secure, and
- Note any action required to be taken with the data from time to time.

1.5 The Council must have a valid legal basis to process personal data. There are six lawful conditions for processing although only five are relevant to public authorities. The six conditions are:

- Legal Contract/contractual necessity – the council can rely on this lawful basis to process someone's personal data to fulfil its contractual obligations to them or because they have asked the council to do something before entering into a contract (e.g. to provide a quote) an example is where a council rents out allotments, or leases property to an individual there is a legal contract between two parties. Another example is where a council has a facility such as a parish hall, the hiring agreement is a legal contract.

- Legal Obligation - the council can rely on this lawful basis if it needs to process the personal data to comply with a common law or statutory obligation – an example is the councillor's Register of Interests which must be on a council website.

- Exercise of public task/public interest – the council can rely on this lawful basis if it needs to process personal data in the exercise of official authority. This covers public functions and powers that are set out in law or to perform a specific task in the public interest set out in law – an example is processing the electoral register for the purposes of a parish meeting or processing planning applications where the council is a statutory consultee.

- Vital Interest – the council is likely to be able to rely on vital interests as its lawful basis if it needs to process the personal data to protect someone's life in an emergency.

- Consent – councils are encouraged not to use this lawful basis for processing if they can use one of the others. An example of where this basis is appropriate is where a council wishes to communicate with residents – it needs their consent to use their personal data to do so. Even though councils may already have a mailing list, good practice is to issue fresh consent forms for completion to ensure that GDPR standards are met.

- Legitimate interest – as public authorities councils cannot rely on legitimate interests as a legal basis for processing personal data.

2.0 PRIVACY NOTICES

2.1 The purpose of a privacy notice is to explain in detail how personal data is collected, stored and used by the council. One notice is to provide this explanation to the public. A second notice is for councillors and employees, informing them of how the council will collect store and use their personal data.

3.0 PESONAL DATA

3.1 Personal data is any information relating to an identifiable living person (a data subject) who can be directly or indirectly identified. The definition provides a wide range of personal identifiers that are classed as personal data, such as name, address, identification (e.g. NI or employee number), location data, e mail or social media tags. The GDPR applies to both automated personal data and data held in paper filing systems.

3.2 Sensitive personal data is described below and needs greater care when being processed as well as a legal basis for doing so, sensitive personal data is information about a person's

- Racial or ethnic origins
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Generic data
- Biometric data
- Sexual orientation

3.3 Councils must process any data lawfully, fairly and in a transparent manner. Only collect and retain personal data for the purposes which it was given. Only keep personal data for as long as it is relevant to do so, where it is kept it must be up to date. Councils must allow anyone who does not wish councils to keep their personal information an opportunity to withdraw any consent they have given. All systems holding personal information must be kept secure.

3.4 Processing information involves the obtaining, collecting, recording, handling, storing, transferring, sharing and deleting of information.

4.0 DATA CONTROLLER

4.1 The Data Controller is the person or organisation who determines the how and what of data processing (i.e. the council). The GDPR introduces a stronger requirement on accountability for data controllers – they shall be responsible for and must be able to demonstrate compliance by providing evidence.

5.0 THE DATA PROCESSOR

5.1 The Data Processor is the person (usually the council clerk or similar officer) or organisation that processes the data on behalf of the controller.

6.0 THE DATA PROTECTION OFFICER

6.1 The GDPR specifies that the Data Protection Officer (DPO) should assist the controller or the processor to monitor internal compliance with the Regulation. The DPO's responsibilities are:

- To understand the nature, scope, context and purposes of the council's processing activities.
- To be involved with the council's decision making and activities which have data protection implications and to make recommendations to council on data protection law compliance.
- To inform, advise and make recommendations to council on data protection laws and the monitor compliance with the data protection law.
- To assist the council in carrying out privacy impact assessments when these are necessary.

7.0 THE INFORMATION COMMISSIONER'S 12 STEPS TO TAKE NOW

7.1 The Information Commissioner has issued a 12-step guide for councils to prepare them for the introduction of GDPR and to ensure compliance with the Regulation. The steps are:

- Awareness – raising awareness of the GDPR within the council
- Information you hold – carrying out an information audit
- Communicating privacy information – putting privacy notices in place

- Individual rights – check procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format
- Subject access requests – update procedures and plan how to handle requests taking account of the new roles.
- Lawful basis for processing personal data – identify the lawful basis for the processing activity
- Consent – review how you seek, record and manage consent
- Children – check whether you need to put in systems to verify individuals' ages and to obtain parental or guardian consent for any data processing activity
- Data breaches – check you have correct procedures in place to detect, report and investigate a personal data breach
- Data protection by design and data protection impact assessments – an impact assessment is required in situations where data processing is likely to result in high risk to individuals e.g. where new technology is being deployed.
- Data Protection Officers – to designate someone to take responsibility for data protection compliance
- International – where the organisation operates in more than one EU member state.

8.0 RECOMMENDATIONS

8.1 That the clerk prepares the necessary policies and procedures to ensure the council is complaint with GDPR on 25 May 2018, in particular to present an Information Audit and the necessary privacy statements to the next meeting.

8.2 At the time of writing this report the requirement for a Data Protection Officer for each parish council has not been clarified. Advice so far received suggests it is necessary for each parish to have a data protection officer, who cannot be the clerk, though it is not clear how this position is filled and by whom.