East Dean & Friston Parish Council

Date:	**3rd May 2018**
Title:	**Report Item 11j – General Data Protection Regulation**
By:	**K Larkin (Parish Clerk)**
Purpose:	**To provide an update on preparations for compliance with the new regulation (effective from 25 May 2018)**
Recommendations:	**To note the report**

At the time of writing the draft GDPR legislation is still in preparation and may be subject to change. With the timescale so tight, the Information Commissioner has issued a statement dated 11 April 2018 giving practical advice, and a checklist of steps to take now. The statement is appended to this report, and the report itself follows the 12 steps of the checklist.

1. **Awareness –** the parish council is aware that the law is changing and will impact on its activities. In November 2017 EDFPC appointed the parish clerk as its Data Controller on the basis of advice received in training. However, **it has since been confirmed that for all local councils the Council itself, as a corporate body, is the formal Data Controller.** This has voided the council's resolution; it means that the responsibility for safeguarding the personal data of individuals who come into contact with the council is shared by all members as well as employees. It is particularly important that data held on mobile devices such as tablets should be password protected or encrypted.

2. **Information the Council holds –** the council must know what personal data it holds, why it is holding it, the legal basis for holding it, where it came from, whether consent is necessary and how it should be protected. The SLCC has helpfully provided a set of model schedules for different sizes of councils, and a local audit is in progress. **This is the area where most work is required.** A full report will be brought to council when it is complete. Briefly, for activities that are undertaken by virtue of being a town/parish council you may not have to gain consent to keep personal information. EDFPC holds the following types of personal data:
   2.1. Electoral Register – a copy is supplied by the District Council and regularly updated. It is held in encrypted form on the office computer, and only current information is retained.
   2.2. Information on councillors – all councillors provide personal information to the council, in the form of a brief CV plus their Register of Interests. The ROI forms are sent to Electoral Services at Wealden. Only current information is retained.
   2.3. Information on employees – information on former employees (CVs, contracts, PAYE details etc.) should be retained for 7 years after they have left. The present

clerk has been in post over seven years and no information is now held on her predecessors.

2.4. Information from hirers of council facilities – the hire form should be revised to state that the information will be retained for a set period, and a consent form and privacy statement should be provided with the hire agreement form.

2.5. Email information service – a list of personal email addresses is kept with the consent of the persons included in it, for the purpose of providing information to residents on council activities, plus other 'official' information e.g. on planned road closures. These general emails have always included an 'unsubscribe' button, but in future **residents must be removed from the list if they do not explicitly opt to be included.** All residents on the list will be contacted accordingly during May 2018 and the list revised. The parish council does not pass on any contact details to third parties without the explicit consent of the individual concerned. This has been a legal requirement under the Data Protection Act for many years.

2.6. Information required for planning applications – the parish council only uses such information as is already put in the public domain by the South Downs National Park Authority. It does not pass on such information.

2.7. Correspondence – it used to be the practice of local councils to keep a great deal of paper correspondence in filing cabinets. This has largely been superseded by email correspondence, and it has become common for councils to archive a large quantity of emails for reference purposes. Paper records do need to be thinned (the county record office does not generally want correspondence), but as paper does not pass out of control as easily as digital records it is suggested that the audit of digital records be prioritised. When the email address of the parish office changed in January 2018 the opportunity was taken to transfer only those contacts that were still 'live' to the new address book. However, digital records must be routinely 'cleansed' to ensure nothing is kept unnecessarily, and further work is required in this area.

2.8. Information about emergency plan volunteers – held as an unpublished Appendix to the Emergency Plan, with the consent of those named.

2.9. Information from contractors – this is not 'personal information' under the terms of the GDPR.

3. **Individuals' Rights –** the council needs a data protection policy setting out the rights individuals have. The council considered two model policies in November 2017, and further drafts have since been refined by official bodies, including the SLCC. A policy needs to be formally adopted.

4. **Communicating privacy information –** privacy notices need to be provided to anyone whose consent is sought for the retention of personal information. The SLCC has provided model notices. [NB: Consent is not usually required for activities that are undertaken by virtue of being a parish council].

5. **Lawful basis for processing personal data –** this should be identified in each case, documented, and explained in your privacy notices. The model data audit schedule (see item 2 above) will record the lawful basis for each type of information.

6. **Subject access requests –** the council should have a procedure for handling requests from individuals who want to know what information the council holds on them, and/or to have it deleted. The SLCC has provided a template request form.

7. **Consent –** the council must review how it seeks, records and manages consent. The SLCC has provided model consent forms.

8. **Data Breaches** – the right procedures must be in place to detect, report and investigate any personal data breach. The SLCC has supplied a model procedure.

9. **Children** – it is unlikely that the parish council will hold data relating to children, but councils where this might arise are asked to contact the SLCC for specific advice.

10. **Data protection by design, and data protection impact assessments –** the key aim of the legislation is to minimise risk to information privacy. Risk can arise through information being inaccurate, out of date, excessive, irrelevant, kept for too long, disclosed to those who the person does not want to have it, used in ways that are unacceptable to or unexpected by the subject, or not kept securely. Again, the SLCC has provided a model Data Protection Impact Assessment.

11. **Data Protection Officers –** the council must designate a Data Protection Officer to take responsibility for compliance. The DPO will not usually have anything to do unless it is claimed that a data breach has occurred. There has been disagreement between official bodies as to whether the parish clerk can or cannot be the DPO. The SLCC says: 'A member of staff can be a DPO provided they have no conflict of interest and meet the other criteria for the position. SLCC believes that in certain circumstances a clerk to a smaller council can be the DPO. Separate guidance on this will be available later'.

12. **International –** organisations which operate in more than one EU member state must find out who is their lead supervisory authority in each jurisdiction (obviously not applicable to EDFPC).

Statement from the Information Commissioner's Office

11th April 2018

The General Data Protection Regulation (GDPR) requires all public authorities to appoint a Data Protection Officer (DPO). The new Data Protection Act (when passed) will define 'public authority', but it is likely to have the same definition that is in the Freedom of Information Act 2000 (FOIA) and therefore includes all councils.

The Information Commissioner is sympathetic to the challenges that appointing a Data Protection Officer (DPO) may pose for parish and town councils, especially those with limited budgets. She has already acknowledged that smaller councils are unlikely to hold large amounts of personal data, and as a result tend to be less prepared for regulatory changes. But regardless of size, if councils hold personal information, from 25 May 2018, the General Data Protection Regulation (GDPR) applies.

The Commissioner has said previously that the GDPR is a journey rather than a destination. She will be looking to councils to demonstrate that they are committed to making progress towards embedding the right processes and procedures. She wants to reassure councils that if they have a positive attitude to finding practical solutions to some of the challenges of implementation, they will find a pragmatic, fair and proportionate regulator.

In the meantime, we recognise that there's still plenty of work parish and town councils need to do to implement the necessary steps to comply with GDPR. We've already provided a lot of tools and support to help with these steps, including our Guide to the GDPR, frequently asked questions, toolkit and helpline for smaller organisations.

We're also committed to working closely with the National Association of Local Councils (NALC) and the Society of Local Council Clerks (SLCC) to consider alternative solutions to the specific issue of appointing DPOs. For example, we see promise in the idea of developing a shared DPO service allowed under Article 37(3). Whilst such a shared service may not be an immediate fix in time for 25 May, it could in the long term enable smaller councils to manage their data protection requirements effectively.