Ettington Parish Council

Date: 14 March 2018

|  |  |
| --- | --- |
| Item 17 Appendix 6 | General Data Protection Regulations |

1. **Introduction**

The General Data Protection Regulations - GDPR (a European Directive) come into force on 25 May 2018 and, as a Public Authority Ettington Parish Council needs to be compliant. Current legislation, The Data Protection Act 1998, will be replaced by The Data Protection Act 2018 in order to reflect the GDPR. The purpose of this paper is to inform the Council on necessary actions to ensure compliance and to report steps taken to date. The Regulations apply to all forms of information which identify or could identify an individual – electronic (including e-mail), paper, photographic etc.

For the purposes of the GDPR the Council is classed as the Data Controller and, as such it is the Council’s responsibility to ensure compliance.

There are a number of appendices and these are listed at the end of the report – it is important that Councillors read these in their entirety.

Sections 2 – 13 summarise the 12 steps to be taken as recommended by the Information Commissioner’s Office – the full document being included in the appendices, together with a position statement, compliance problems and resource implications.

1. **Awareness**

To make decision makers aware of the GDPR and its impact on the organisation in order that they are aware of the impact and any likely compliance problems and the resource implications.

*Position Statement:* This report aims to raise awareness and Councillors should ensure they are familiar with it and its appendices.

*Compliance Problems:* Councillors not reading the report and appendices.

*Resource Implications:* Councillors’ time.

1. **Information You Hold**

Document what personal data you hold, where it came from and who it is shared withwhich may necessitate an information audit.

*Position Statement:* Not compliant - audit form prepared (Appendix 1)

*Compliance Problems:* None envisaged

*Resource Implications:* A substantial amount of Clerk’s time

1. **Communicating Privacy Information**

Review current privacy notices and put in place a plan for making any necessary changes.

*Position Statement:* Not compliant

*Compliance Problems:* None envisaged

*Resource Implications:* Minimal Clerk’s time to research suitable wording and commence using.

1. **Individuals’ Rights**

Check procedures to ensure all rights are covered.

*Position Statement:* Not compliant - Included in audit (Appendix 1)

*Compliance Problems* None envisaged

*Resource Implications:* Included in 3 above

1. **Subject Access Requests**

Update procedures and plan how to handle requests in line with the new rules:

*Position Statement:* Not compliant – will need to write policy/procedure

*Compliance Problems:* None envisaged

*Resource Implications:* A moderate amount of Clerk’s time.

1. **Lawful Basis for Processing Personal Data**

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

*Position Statement:* Not compliance – included in audit (Appendix 1)

*Compliance Problems:* None envisaged

*Resource Implications:* included in 3 above.

1. **Consent**

You should review how you seek, record and manage consent and whether you need to make any changes.

*Position Statement:* Not compliant – need to read the detailed guidance provided by Information Commissioner’s Office and include in policy/procedure.

*Compliance Problems:* Currently no permissions sought.

*Resource Implications:* Considerable amount of Clerk’s time.

1. **Children**

You should start thinking about whether you need to put sysems in place to veryify individuals’ ages and to obtain parental or guardian consent for any data processing activity.

*Position Statement:* Not compliant

*Compliance Problems:* Will need to a) identify ages of all young people on circulation list for Youth Council and b) where necessary ask them to pass a permission form to their parent. Experience shows young people need a lot of ‘chivvying’ to undertake actions.

*Resource Implications:* Has the potential to require a considerable amount of Clerk’s time.

1. **Data Breaches**

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

*Position Statement:* Not compliant – included in audit

*Compliance Problems:* None envisaged

*Resource Implications:* Included in 3 above.

1. **Data Protection by Design and Data Protection Impact Assessments**

GDPR makes privacy by design and express legal requirement and, in certain circumstances to undertake Privacy Impact Assessment.

*Position Statement:* Not compliant – need to read the ICO’s Guidance on PIAs.

*Compliance Problems:* None envisaged

*Resource Implications:* A moderate amount of Clerk’s time.

1. **Data Protection Officers**

As a public authority the Council must appoint a DPA who takes proper responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively.

*Position Statement*: Not compliant

*Compliance Problems*: The Society of Local Council Clerks and the National Association of Local Councils have identified, to Government, that this could be problematic for Parish Councils with only one employee who, processes all data.

*Resource Implications:* May require the appointment of an additional staff member/ contracting with an organisation to undertake this role.

1. **International**

Only relevant if the organisation carried out cross-border processing.

*Position Statement:* Not applicable

*Compliance Problems:* N/A

*Resource Implications:* N/A

1. **Action Required:**
2. To read the report and, in particular, the Appendices to it;
3. To consider whether the Position Statements, Compliance Problems and Resource Implications for sections 2-13 are realistic
4. To consider whether the audit (Appendix 1) is fit for purpose
5. To consider whether a Councillor be appointed to oversee the work of the Clerk in respect of the GDPR
6. To raise any issues or queries

Appendix 1 Audit – must read

Appendix 2 Workplan – must read

Appendix 3 Preparing for the General Data Protection Regulations – must read

Appendix 4 SLCC Presentation – very useful

Appendix 5 NALC GDPR February 18 – very useful

Appendix 6 DPO Guidance – for information

Appendix 7 A Guide to ICO PERC Audits – for information

Appendix 8 SLCC Webinar Presentation – very useful

**Glossary**

**Consent** is a positive, active, unambiguous confirmation of a data subject’s agreement to have their data processed for a particular purpose. Consent must be easy to withdraw and must be freely given, provided on an opt-in basis rather than an opt-out.

**Data Controller:** The Organisationthat determines the how and what of data processing (the Parish Council)

**Data Processor:** Anyone who processes data – this will, in most situations be the Clerk but could be Councillors (eg in e-mails).

**Data subject** is the person about whom personal data is processed

**Personal data** is information about a living individual which is capable of identifying that individual, eg a name, e-mail, address or photo

**Privacy Notice** is a notice from a data controller to a data subject describing how personal data will be used and what rights the data subject has.

**Processing** is anything done with/to personal data (obtaining, recording, adopting or holding/storing)personal data

**Sensitive personal data** is also described in the GDPR as ‘special categories of data’ and is the following types of personal data about a data subject: racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health condition; sexual life or orientation; genetic data and biometric data.

**Data Protection Officer**: The personappointed to have responsibility for ensuring the GDPR is complied with.