GENERAL DATA PROTECTION REGULATION (GDPR 2018)

Sample Impact Assessment.

1. PURPOSE OF THE ASSESSMENT.

The assessment summarises the impact on the Council of the new General Data Protection Regulation (GDPR) which comes into force on 25 May 2018 and the associated risks of non-compliance. This report gives details of required actions and provides an initial action plan aimed at achieving compliance with the new requirements.

2. BACKGROUND INFORMATION

2.1 On 25 May 2018, the GDPR will come into force across the European Union (EU), replacing existing data protection laws. The GDPR will increase the rights of individuals over their personal data and tighten the obligations of all organisations to comply with new rules concerning the management of personal information.

2.2 While the UK decision to leave the EU means that the GDPR will no longer apply to the UK in the longer term, the GDPR will apply to the UK directly until the UK is no longer a member. Furthermore, the Government has confirmed that the UK will opt into the GDPR. Following this commitment, the UK Information Commissioner's Office (ICO) has stated that, whatever the outcome of the negotiations to exit the EU, UK data protection standards will be equivalent to the EU GDPR framework in order not to create any block on trade with the EU single market.

3. IMPACT ON COMBE MARTIN PARISH COUNCIL (CMPC)

3.1 CMPC handles and stores reasonable amounts of personal data as part of its routine service to its parishioners / customers. The volume of data processed and retained is constantly increasing. Good data protection is therefore fundamental to high standards of customer service and the effective operation of the Council's business. Personal data is an asset owned by the customer as must be treated accordingly.

3.2 The GDPR significantly increases the data protection obligations on the Council and although existing data protection procedures are in place, these require extensive review and revision in order to achieve compliance with the GDPR framework.

3.3 Many of the GDPR's main concepts are the same as those in the current Data Protection Act 1998 (DPA). This means that the CMPC's current approach to compliance under existing law will remain valid. However, new elements and significant enhancements within the GDPR will need to be taken account of and prepared for.

3.4 The most significant addition is a new 'accountability' requirement. Parish Councils will need to be able to demonstrate compliance with the GDPR principles, for example, by maintaining documentation on decisions about why personal information is being processed. Another important change is vastly increased fines for those organisations that fail to comply with GDPR or permit data breaches. For serious breaches organisations can be fined up to €20million. For less serious breaches or for failing to keep records the fine can be up to €10million.

3.5 The requirements of GDPR are extensive and complex. The ICO has produced a checklist highlighting the specific steps that should be taken to meet the requirements. This checklist should be used to develop an initial action plan to ensure compliance by May 2018. As part of the programme training should be given to Councillors on the GDPR impact and implementation to ensure the Council achieves compliance.

3.6 The action plan will require a reasonable amount of work to prepare for implementation and given the limited resources available within the CMPC office, this should be taken in to consideration during the budget setting process and monies set aside to ensure compliance. Following on from implementation there will be ongoing work to manage the Council's data in compliance with GDPR requirements which may not be achievable from within existing resources.

4 STEPS TAKEN TO DATE

4.1 To demonstrate compliance the Council must:

- Implement technical and organisational measures that demonstrate compliance. These include data protection policies, staff and Member training, internal data processing audits.
- Maintain relevant documentation on processing activities.
- Appoint a Data Protection Officer (DPO) (a new statutory role).
- Implement measures that meet the principles of data protection by design including, data minimisation, using artificial identifiers e.g. replacing a name with numbers and transparency.
- Implement data protection privacy impact assessments.

4.2 Under current DPA arrangements, the ICO only respond reactively to data breaches. It must be noted that, following implementation of the GDPR, the ICO will implement a proactive inspection regime to monitor compliance. Enforcement action could follow any breaches arising during inspections.

4.3 As noted above, a DPO must be appointed and there is considerable flexibility as to how this requirement is met. It is a matter for each council to determine who should act as DPO and what level of knowledge and expertise they require as they have the best knowledge of the personal data they process, any risks involved and the wider context in which they operate. In order to avoid a conflict of interest a DPO should not determine the purpose or manner of processing personal data. Provided that a Parish Council is satisfied that the Clerk does not do this then they could act as the DPO, however this is highly unlikely. It is also possible appoint someone external to the council and the possibility of sharing a person between parish councils or sharing with the district council or other principal local authority should be explored.