Agenda item 5

For decision - Approval of policies to implement the Data Protection Act (DPA) 2018 and the General Data Protection Regulation (GDPR)
Author: Paul Wynne, Town Clerk

Summary

This report summarises the actions FTC is taking to adhere to the DPA and the GDPR. It asks Cllrs to note the data audit report and approve a new Data Protection Policy and Privacy Policy.

Background

The GDPR forms part of the data protection regime in the UK and is a consequence of the new Data Protection Act 2018 (DPA 2018). The main provisions of the DPA, like the GDPR, apply from 25 May 2018. Advice from the Information Commissioner's Office (ICO) is that local councils need to be on a journey towards compliance rather than comply by this date.

There are principles that lie at the heart of the GDPR. These are in the Data Protection Policy at Appendix 1. They don't give hard and fast rules, but rather embody the spirit of the general data protection regime. It is ambiguous by design. What is not available from the Information Commissioner's Office (ICO) are model policies, although latterly the SLCC and NALC have produced checklists and a model privacy policy. This is lack of model documents from the ICO is understandable, given that the regulations apply to all organisations from massive multinationals through parish councils with perhaps one part time employee to tiny charities with no employees and trustees with usually no expertise in data protection.

What it does mean is that to be confident that FTC is holding personal data lawfully, we have audited ourselves to find out what data we've got and we need to draft policies and procedures pertinent to our situation. What we are confident about was that we were aware of the need to hold personal data securely and that consent was given when required. The new regulations, however, tighten up the consent procedure.

The big change in the GDPR is that the consent of individuals changed from having to "opt out" to one of "opting in". This means that in the past, if you received a newsletter, for example, from an organisation, you had to ask them to remove you from their mailing list. Now, the organisation must ask you if you want to continue to receive the newsletter. This is why we've all had many emails asking us this question from organisations we've never even heard of.

If you have said you want to receive the newsletter and the organisation holds your personal data securely, generally, the organisation is compliant. There are other lawful reasons for organisations to hold personal data that do not require consent. These include FTC holding personal details of Cllrs. FTC has to hold this information and publish it on the website in the form of declaration of interests. Similarly, as an employer, FTC must hold personal details of

staff. The main question on the latter is not whether the data should be held but is it held securely?

In summary, the GDPR asks us to identify the personal data we hold, ensure that it is held with consent or for other lawful reasons, that personal data is held securely and only for as long as it needs to be held.

What FTC has done so far

Last year, we commissioned DP Assist to audit our personal data to get an understanding of what personal data we held and whether it was held legally and securely (under the new GDPR). DP Assist are a data protection training and consultancy organisation that provided FTC staff training in 2016 on compliance and best practice around data protection legislation.

DP Assist carried out the audit by interviewing all staff about what data they held and where they held it. DP Assist have since drafted a report with recommendations that, when implemented, will ensure we comply with the GDPR (this is a confidential document and available to Cllrs only, on request). In addition, we have drafted with DP Assist's advice a Data Protection Policy (Appendix 1) and a Privacy Statement (Appendix 2). DP Assist are also drafting numerous policies and procedures that deliver the recommendations in the main report. There are also actions that FTC needs to implement and it is proposed to review progress at this time next year.

So that we can manage personal details better in future, it is expected that much of the data different members of staff hold will be moved to the new Customer Relationship Management system this year. Rachel Griffin is leading on this.

Recommendations

1. Note the Audit report including its recommendations (confidential document)
2. Approve the Data Protection Policy at Appendix 1
3. Approve the Privacy Statement at Appendix 2
4. Note that the Audit Report is being implemented and that a review of progress will be tabled at the Council Matter meeting in July 2019.