

**Policy and Finance Committee**

---

**Date:** 17 June 2019

**Title:** Data Protection

**Purpose of the Report:** To receive an update regarding data protection and consider arrangements for 2019-2020.

**Contact Officer:** Sarah Sandiford, Head of Democratic and Central Services

---

<b>Corporate Objective/s</b>	<b>To consolidate processes and procedures, ensuring operational efficiency.</b>	
<b>Implications:</b>		
<b>Financial</b>	√	Potential cost of £150 to be met from the Professional Fees budget 12/4384
<b>Human Resources</b>		
<b>Operational/Service delivery</b>	√	To ensure adequate resource is in place to support data protection requirements in accordance with the Data Protection Act 2018.

**1. RECOMMENDATION**

- 1.1 To consider whether to renew the existing agreement for external Data Protection Officer services to the Town Council, at a cost of £150 per annum (to be funded from the Professional Fees budget).**

**2. BACKGROUND**

- 2.1 During the year 2017-2018, the Town Council undertook a significant number of actions in preparation for the introduction in 2018 of the mandatory General Data Protection Regulation (GDPR). A European ruling, GDPR introduced a number of new requirements in respect of individual's rights concerning their personal data.
- 2.2 As a result of guidance issued by the Information Commissioners Office (ICO), the National Association of Local Councils (NALC) and the Society of Local Council Clerks (SLCC), actions undertaken by the Council included the following:

- Creation of a register of personal data held and the legal basis for the processing of such data
- Intensive staff training over a period of months
- Development of new policies including ICT Security, Information and Data Protection, Removeable Device Policy, Information Security Breach processes, Subject Access Request processes.
- Initial audits by two external consultants
- Development of a number of Privacy Notices
- Adoption of a Document Retention Policy and a subsequent period of sorting and securely destroying personal data no longer required to be held by the Council.

2.3 In the run-up to the GDPR deadline and introduction of the new Data Protection Act in May 2018, it was understood that all organisations would need to appoint a named Data Protection Officer. Sector guidance was that it was inappropriate to appoint the Clerk into the role of DPO due to the potential for conflict of interest.

2.4 Following research into the available options, it was agreed by Council to appoint an external Data Protection Officer. The appointment made was The Local Council Public Advisory Service (LCPAS) which offered a sector-specific service to parish councils at a cost of £500 for a year, including an audit visit.

### **3. UPDATE**

3.1 In September 2018, an audit visit was undertaken by LCPAS and a positive verbal report given. However, the written report was never received.

3.2 The project to securely destroy a significant amount of archived data has continued with monthly collections of waste paper to be shredded.

3.3 New forms have been developed for use in all service areas, taking into account the need for consent to hold personal data.

3.4 Following a number of attempted contacts to seek consent to continue to hold personal data, any electronic mailing lists have been edited.

3.5 The Town Council website has been restructured to ensure that the site itself retains no personal data (for example, from submitted enquiry forms).

3.6 Staff training and reminders are ongoing.

3.7 In the year since the introduction of GDPR and the Data Protection Act, the Town Council has received no Subject Access Requests and has not been subject to any data or information breaches.

- 3.8 As a result of lobbying by NALC, the Data Protection Act ultimately exempted parish councils from the need to appoint an external Data Protection Officer. This was in recognition of the fact that the majority of parish councils are very small with perhaps only one member of staff, the Clerk, and with limited funds.

#### **4.0 CONSIDERATIONS**

- 4.1 The Town Council has now reached the end of the first year period of the contract with LCPAS for outsourced Data Protection Officer arrangements. The Committee is asked to consider whether to renew the agreement for a further year.
- 4.2 The fee in 2018-19 to parish councils was £300, or £500 if an audit visit was to be included. The fee for 2019-20 has been reduced to £150. In recognition that the Town Council never received its written report from the September 2018 visit, LCPAS has agreed to provide this service free of charge in the next year. The renewal fee for 2019-2020 would therefore be £150.
- 4.3 Costs for the service could be met from the existing revenue budget line "Professional Fees".
- 4.4 Compliance with legislation, including data protection and Freedom of Information, falls within the remit of the Head of Democratic and Central Services. However, it is suggested that an external appointment for DPO services would provide an independent view, in the way that the internal auditor provides a double check and gives assurance to Council that proper practices are being adhered to.
- 4.5 LCPAS within its service offer also provides a first point of contact for dealing with any security breaches or Subject Access Requests. See Appendix A for the list of services included.
- 4.6 LCPAS is the only known sector-specific provider of such services. From previous research, data protection services offered within the private sector may be significantly more expensive.

#### **5.0 CONCLUSIONS**

- 5.1 The Committee is asked to consider whether to renew the existing arrangement with LCPAS for outsourced data protection services.

## **Appendix A: Local Council Public Advisory Service data protection service for town and parish councils**

Full service details:

Each Council will receive a Service Contract

We will:

- Inform and advise the Council and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; assist with training staff and assist with conducting internal audits.
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, members of the public etc).
- Provide privacy notices and consent forms and policies at no additional cost
- Monitor ongoing compliance by a variety of methods
- Provide up to date guidance including unlimited helpline calls and emails
- Help manage access requests or requests made under the other powers for individuals
- Provide IT recommendations and identify solutions for data security