**MUNICIPAL YEAR 2018/2019 REPORT NO. 188**

| | |
|---|---|
| **Agenda – Part: 1** | **Item: 7** |
| **Subject: Data Protection Officer Report**<br><br>**Wards: All**<br>**Non Key** | |
| **Cabinet Member consulted: Cllr Mary Maguire** | |

**MEETING TITLE AND DATE:**
Cabinet – 12 March 2019

**REPORT OF:**
Acting Director Customer Experience and Change

Contact officer and telephone number:

Steve Durbin, Data Protection Officer 020 8379 2504

E mail: Steve.Durbin@enfield.gov.uk

## 1. EXECUTIVE SUMMARY

Following the completion of the project to implement changes required by the new General Data Protection Regulations (GDPR) which became law on 25 May 2018, work has now transferred to 'business as usual'.

Three data breaches were reported by the Data Protection Officer (DPO) to the Information Commissioner's Office (ICO) between October 2017 and this report. All have been closed without further action by the ICO, and guidance from the ICO has been actioned by the teams involved.

The council's compliance continues to improve and as further guidance is issued by the ICO the DPO will ensure it is publicised. Key areas where compliance improvement is still needed are:

- Early consultation by staff with the DPO on data use
- Use of live data for purposes for which it was not collected
- Compliance with requirements for data processing or sharing agreements
- Public forms data protection statements
- Timescales for response to subject access requests (SARs); requests to exercise rights under GDPR and FOIA requests

The DPO will continue to raise awareness, understanding and compliance within the council.

## 2. RECOMMENDATIONS

2.1 That the Cabinet note the report.

## 3. BACKGROUND

3.1 The tasks of the DPO are defined in the legislation. The ICO summarises them as:

- to inform and advise you and your employees about your obligations to comply with the GDPR and other data protection laws;
- to monitor compliance with the GDPR and other data protection laws, and with your data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor, data protection impact assessments;
- to cooperate with the supervisory authority; and
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

3.2 This report constitutes part of these tasks and is required by law (see section 5).

3.3 The DPO made a detailed report to the Executive Management Team, which is summarised for the Cabinet at Appendix A.

## 4. ALTERNATIVE OPTIONS CONSIDERED

4.1 The provision of an annual report is a required action by the law, and as such no alternative option was considered.

## 5. REASONS FOR RECOMMENDATIONS

5.1 The Data Protection Act 2018 adopted and adapted the Applied General Data Protection Regulation 2016/EU679 into UK law.

5.2 Article 38 (3) of the General Data Protection Regulation requires that "…The data protection officer shall directly report to the highest management level of the controller…"

5.3 This report fulfils the obligation in 5.2 above and follows the guidance issued by the Article 29 Working Party on the role of the Data Protection Officer.

## 6. COMMENTS FROM OTHER DEPARTMENTS

### 6.1 Financial Implications

There are no financial implications to this report.

.

### 6.2 Legal Implications

This report makes reference, in paragraph 5, to the legislative basis for the appointment and role of a Data Protection Officer within the Council. Article 39 of the GDPR sets out the tasks of the DPO as listed above in paragraph 3.1.

In the UK, the GDPR has been implemented by the DPA 2018, the main provisions of which also apply from 25 May 2018. The GDPR and the DPA 2018 must be read together and the DPA 2018 assumes familiarity with the GDPR. The DPA 2018 serves several functions, as it:

- Replaces the Data Protection Act 1998.
- Incorporates the GDPR into UK law.
- Fills in the gaps (the domestic derogations) in the GDPR.
- Addresses data processing in law enforcement and the intelligence services (which are covered by the Law Enforcement Directive ((EU) 2016/680))
- Is intended to ensure that on leaving the EU, the UK has an "adequate" data protection regime to that of the EU

For all tasks, the DPO is required to have due regard for the risks associated with the processing operations.

In accordance with the DPO's tasks, this report sets out a summary record of the monitoring of compliance at Appendix A.

The Council, not the DPO, is responsible for implementing appropriate technical and organisational measures to ensure that it is in compliance with the GDPR (Articles 24 and 28). The Article 29 Working Party (WP29) Guidance - now known as the European Data Protection Board - makes it clear that the DPO has no direct liability for an organisation's failings, as does the ICO who notes that while the DPO plays a crucial role in helping an organisation to fulfil its data protection responsibilities, they are not personally liable.

Where the Council disregards the advice of the DPO, the WP29 Guidance also recommends that this is noted in Data Protection Impact Assessment documentation, along with the justification as to why this advice was not followed.

### 6.3 Property Implications

There are no property implications of this report.

## 7. KEY RISKS

This report is required by law and the risk of not completing it would be non-compliance.

## 8. IMPACT ON COUNCIL PRIORITIES – CREATING A LIFETIME OF OPPORTUNITIES IN ENFIELD

### 8.1 Good homes in well-connected neighbourhoods

No impact

### 8.2 Sustain strong and healthy communities

Compliance with law and a strong enforcement of rights of service users will assist in strong and healthy communities.

### 8.3 Build our local economy to create a thriving place

No impact.

## 9. EQUALITIES IMPACT IMPLICATIONS

Good Data Protection is essential for adhering to equalities legislation – collecting data on protected characteristics and analysing it within the protections of the Data Protection Legislation. We must also ensure that to the extent we are not perfectly compliant, this does not disproportionately impact some individuals.

## 10. PERFORMANCE AND DATA IMPLICATIONS

Performance in meeting SLAs and data breaches in this area will continue to be monitored closely through the council's Information Governance Board and will feature in future reports.

## 11. PUBLIC HEALTH IMPLICATIONS

There are no public health implications.

**Background Papers**
None

**Appendix A Summary of EMT Report of the Data Protection Officer.**

## Business Requests

A Service Level Agreement was made in February 2018 that 80% of all Data Protection Officer emails would be responded to with within 1 day, and 100% within 2 days. This SLA was met, with the following email volumes (note that not all emails required responses e.g. emails that simply thanked the DPO for the advice):

| | ***Corporate*** | | ***Schools*** | | ***Uncategorised (i.e. mix of Corporate & Schools)*** | | ***Overall*** | |
|---|---|---|---|---|---|---|---|---|
| **Date** | **Received** | **Sent** | **Received** | **Sent** | **Received** | **Sent** | **Received** | **Sent** |
| Feb-18 | 19 | 6 | 31 | 14 | 771 | 305 | 821 | 325 |
| Mar-18 | 20 | 7 | 57 | 38 | 865 | 391 | 942 | 436 |
| Apr-18 | 26 | 27 | 3 | 77 | 448 | 180 | 477 | 284 |
| May-18 | 28 | 13 | 306 | 209 | 832 | 442 | 1,166 | 664 |
| Jun-18 | 59 | 50 | 97 | 89 | 555 | 291 | 711 | 430 |
| Jul-18 | 57 | 46 | 143 | 87 | 455 | 190 | 655 | 323 |
| Aug-18 | 137 | 74 | 43 | 15 | 442 | 181 | 622 | 270 |
| Sep-18 | 46 | 19 | 47 | 39 | 383 | 165 | 476 | 223 |
| Oct-18 | 54 | 36 | 150 | 51 | 316 | 201 | 520 | 288 |
| Nov-18 | 75 | 48 | 70 | 59 | 458 | 106 | 603 | 213 |
| Dec-18 | 44 | 19 | 20 | 14 | 266 | 228 | 330 | 261 |
| **Total** | **565** | **345** | **967** | **692** | **5,791** | **2,680** | **7,323** | **3,717** |

Staff tend to use personal email accounts (e.g. for members of the team) for DPO queries, which do not then have the SLA and we cannot easily separate schools and corporate issues. Only emails in this category *direct to the DPO's personal mailbox* have been included, and are marked above as "uncategorised".

The DPO and the team additionally attended a large number of advisory meetings with both schools and council staff. Q&A sessions have also been run for both schools and council staff. Feedback on these sessions has been very positive and it has been agreed to run these on a quarterly basis as part of the DPO's "inform and advise" responsibility.

## Data Breaches

There have been 31 breaches since October 2017 that have been recorded as breaches of the data protection legislation i.e. that involved loss or exposure of personal data.

Of these, three have been self-reported to the Information Commissioner as required by the law when there is a significant risk to rights and freedoms of individuals. Comparisons between authorities are difficult as there was no obligation to report before May 2018, but there were 263 breaches by councils

for Q1 2018/9 reported to the ICO, which equates to an average of 2.5 per council per year, suggesting Enfield Council is around the average.

The total of 31 is harder to compare as there is no recent data, no obligation to publish and reporting policies in authorities differ. A Big Brother Watch survey in 2015 suggested an average of 19 breaches per year across all local authorities, but as awareness has risen so has reporting; one council of similar size to Enfield, in a more recent FOI request reported an average of 67 per year over the past 3 years.

## Overall Compliance

### Training and Awareness

Over 80% of people registered on iLearn and active on the council's IT systems have undertaken the GDPR training. This is a considerable improvement on the position for the previous training and demonstrates good management commitment to the process.

The DPO now runs quarterly sessions for both council and school staff to bring and workshop questions; these have been very well attended and feedback has been positive. It is intended that this will continue. The DPO also sends out feedback from these sessions to all staff and schools so that knowledge is spread, and publishes questions asked on SharePoint for internal viewing.

Some staff, despite training, are still not aware of the need to consult the DPO on changes or new uses of data. This is generally being picked up when new projects come for initiation to the Customer Experience and Change Division, but there may still be gaps where projects are not involved. The manager awareness training for GDPR does include this, but we recommend that all departmental level meetings have an item regarding new/changed data use as a regular review.

The data catalogue (the GDPR workbooks, part of our detailed Article 30 compliance) is still subject to improvement. In particular, there are still gaps in terms of ensuring that public forms are clear on the data uses and law – this was de-emphasised during the project as other compliance issues were higher priority. Work is ongoing to correct this with the data owners. As all items in the data catalogue are to be reviewed annually, we have started this process and a focus will be to address this shortcoming. All data owners will be receiving emails shortly asking them to engage, and in cases where the data owner has left or changed responsibility this will be escalated to appropriate service heads.

Many areas of the council are still using live data for purposes for which it was not collected, in particular internal system testing. A project is in place to start mitigating the risk by anonymising the data, but it remains a key issue. The project is currently expected to take 8-12 months to complete, having started in October 2018.

The timescales for responses to FOIA and SAR requests have been a problem within the council for a considerable time, and the shortening of the SAR and rights deadlines may have further exacerbated this; coverage of this issue will be made by the Complaints & Information team who handle the requests, and FOIA performance is reported quarterly to Cabinet.