MUNICIPAL YEAR 2019/20 REPORT NO. 36

Agenda – Part:	**Item: 6**
Subject: IGB annual report including GDPR implementation update. **wards: all** **Key Decision No :n/a**	
Cabinet Member consulted:	

MEETING TITLE AND DATE:
Audit Committee June 19th, 2019

REPORT OF:
Director of Law and Governance
Jeremy Chambers
Contact officer and telephone number:

Jayne Middleton-Albooye 0208379 6431

E mail: Jayne.middleton-albooye@enfield.gov.uk

1. EXECUTIVE SUMMARY

This report updates Audit Committee on the work of the Information Governance Board (IGB) and provides assurance that the Council is complying with its statutory duties in respect of information governance and access to information.

IGB is also responsible for considering any Data Protection breaches or Information Commissioner's Office (ICO) referrals, and this report and its attachments summarise matters that have come to IGB (Breaches calendar year 2018 and ICO referrals financial year 2018/2019).

IGB oversaw the implementation of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) in the Council, and this report notes the internal audit of compliance as having reasonable assurance.

2. RECOMMENDATIONS

Audit Committee is asked to note:

1. The work of IGB for the financial year 2018/19
2. Compliance with GDPR and DPA 2018 in first year of implementation
3. The annual Corporate and Statutory Complaints and Access to Information reports which will be taken to Cabinet.

3. BACKGROUND

3.1 The current Information Governance Board (IGB) has been meeting since September 2017. The IGB meets monthly and its membership comprises officers of the Council who have information governance, data security, access to information and data analysis and performance within their remit, across all departments of the Council. The Chair of IGB takes regular reports to Assurance Board and to EMT.

3.2 The GDPR implemented in the UK in May 2018 together with the DPA 2018 placed new obligations on the Council as a data controller and, in some cases as data processor, and most importantly increased the level of fines that could be imposed as a sanction for breaches to 4% of annual worldwide turnover or €20 million. The risk of such huge financial sanctions as well as the reputational risk means that compliance with data protection and information governance law and regulations has never been more important.

3.3. The GDPR required public sector organisations such as the Council to appoint a Data Protection Officer (DPO). DPOs assist in monitoring internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

- The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.
- DPOs can help demonstrate compliance and are part of the enhanced focus on accountability.

3.4 An important part of evidencing compliance with GDPR is training. Online training for data owners and training generally on GDPR requirements are available and mandatory for all staff on MI Portal. A Cyber Security module is also mandatory and part of the role of IGB has been to raise awareness of training and to increase uptake. IGB also review all relevant policies and procedures on an annual basis.

3.5 Internal Audit of GDPR compliance gave an overall reasonable assurance level. IGB will consider the internal audit report as part of its work programme.

The overall findings were as follows:
Medium risk:

- A lack of a centralised view on the retention and disposal of paper
  A lack of GDPR safeguards on all relevant systems and duplicating data
- A lack of employee awareness on data retention responsibilities
- Risk rating for data breaches not defined

Low risk:

- Unclear plan for the restructuring of the Data Protection Office (DPO)
- Process for maintaining Records of Processing Activity not clear
- • A lack of Legal review over the Records of Processing Activities

3.6 Reporting of Data breaches.

All security incidents are logged by the Security Team and reviewed at the monthly SWG meeting. Potential personal data breach incidents are reported immediately to the DPO. Data loss incidents are reported to IGB monthly for separate review. The security team also log incidents on behalf of Enfield schools as part of an existing contractual requirement.

Annual Security Incidents Report 2018	
Total Reported Incidents	**128**
Disclosure in error	**49**
Lost data / hardware	**23**
Emails (Spear phishing / Spoofing)	**38**
Physical Security Failure	**1**
Stolen data / hardware	**3**
Technical failure	**13**
Unauthorised Access	**1**

There were 128 recorded incidents in 2018, of most concern are data loss incidents which involve loss or exposure of personal data. There have been 59 breaches since November 2017 (to end of 2018) 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.

Of these:

- 1 included breaches of procedure as the contractor involved had not had data protection issues included in their contract
- 1 was staff misuse which was subject to a disciplinary investigation
- 1 was accidental misaddressing of data sent by recorded post which was not then recovered.

Organisational Learning and mitigating actions from the breaches includes:

- Ensuring that all contracts with contractors contain adequate GDPR clauses.
- Most disclosure in error incidents are caused by individuals inadvertently sending emails to the wrong person. Those officers who do this repeatedly are required to repeat the Cyber Security training,

and to consider switching off the cache data tool that enables names to automatically populate the e-mail address line.

- All hardware devices (laptops/ tablets / mobile phones) are encrypted by default and are immediately disconnected from the network as soon as the loss is reported.
- Reminders of the policies and where to find the policies, and reminders of the process for reporting.
- The amount of spoofed emails and phishing should be mitigated by the implementation of an improved O365 Secure mail solution and improved protection on the mail gateway.
- The cyber security training has been completely updated to account for the new data protection requirements and new threat landscape.

3.7 Access to Information and response to Corporate and Statutory Complaints.

Three annual reports are attached to this report. These reports detail the Council's performance in responding to requests for information under the Freedom of Information Act 2000 (FOIA), Data Protection Act 2018 and to either Corporate Complaints or Statutory complaints. A central team responds to, and co-ordinates the responses of the Council, and liaises with the regulator. The team has been operating under an interim model for the financial year 2018/19, but from 1st June 2019 will be operating a new model which will result in an increase in the performance of the Council in responding to Complaints and Access to Information within the deadlines.

4. ALTERNATIVE OPTIONS CONSIDERED

No alternatives were considered, it is good practice for Audit Committee to consider the work of IGB annually.

5. REASONS FOR RECOMMENDATIONS

The recommendations are for noting only so that the Audit Committee has knowledge of the work of IGB and can receive assurance that the Council is complying with its obligations in respect of information governance and data security.

6. COMMENTS FROM OTHER DEPARTMENTS

6.1 Financial Implications

There are no direct financial implications arising from the recommendations in this report.

6.2 Legal Implications

There are no direct legal implications. It is good governance for Audit Committee to consider the work of the Information Governance Board

and to note the first-year progress of the implementation of the GDPR and the DPA 2018.

6.3 Property Implications

n/a

7. KEY RISKS

n/a

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

8.1 Good homes in well-connected neighbourhoods

The Council's response to Complaints and requests for information assists the Council in improving its services.

8.2 Sustain strong and healthy communities

The work of the IGB helps to promote an open and transparent Council.

8.3 Build our local economy to create a thriving place

The work of IGB helps to protect the Council from Data breaches which could lead to financial and reputational loss for the Council.

9. EQUALITIES IMPACT IMPLICATIONS

n/a

10. PERFORMANCE AND DATA IMPLICATIONS

The performance of compliance with GDPR, FOIA and Corporate and Statutory Complaints is monitored closely to seek to improve meeting statutory deadlines, improve services to the residents and to provide organisational learning from concerns that are reoccurring.

11. HEALTH AND SAFETY IMPLICATIONS

n/a

12. HR IMPLICATIONS

n/a

13. PUBLIC HEALTH IMPLICATIONS

n/a

Background Papers

Appendices

Corporate Complaints and Access to Information Annual report
Statutory Complaints Annual report - Children's
Statutory Complaints Annual report - Adults