

<b>CITY OF WOLVERHAMPTON COUNCIL</b>	<b>Cabinet (Performance Management) Panel</b> <b>24 June 2019</b>
--	--

<b>Report title</b>	Information Governance Quarter Four Performance and General Data Protection (GDPR) Update Report		
<b>Decision designation</b>	AMBER		
<b>Cabinet member with lead responsibility</b>	Councillor Sandra Samuels OBE Governance		
<b>Key decision</b>	No		
<b>In forward plan</b>	Yes		
<b>Wards affected</b>	All		
<b>Accountable Director</b>	Mark Taylor, Deputy Managing Director		
<b>Originating service</b>	Information Governance		
<b>Accountable employee</b>	Anna Zollino-Biscotti	Information Governance Manager and Data Protection Officer	01902555166
	Tel		<a href="mailto:Anna.zollino-biscotti@wolverhampton.gov.uk">Anna.zollino-biscotti@wolverhampton.gov.uk</a>
<b>Report to be/has been considered by</b>	Strategic Executive Board Information Governance Board	4 June 2019	18 June 2019

#### Recommendations for decision:

The Cabinet (Performance Management) Panel is recommended to:

1. Review the quarterly progress update on the General Data Protection Regulation (GDPR).
2. Review the quarter four performance for Information Governance.

## **1.0 Purpose**

- 1.1 To provide an update on the Information Governance performance figures for quarter four 2018-2019.
- 1.2 To provide a quarterly update on the work currently being undertaken by the Information Governance (IG) team and directorates following the implementation of the General Data Protection Regulation (GDPR).

## **2.0 General Data Protection Regulation**

### **Background**

- 2.1 On 14 April 2016, the EU Parliament approved the General Data Protection Regulation. In the following October, the Government confirmed that it would implement the GDPR in the UK and that the UK's decision to leave the EU would not affect the commencement of the GDPR. The new regulations have replaced the Data Protection Act 1998 and the Information Commissioner's Office (ICO) will continue to be the supervisory authority for the UK.
- 2.2 In April 2017, the Government issued a consultation document to consider the derogations (exemptions) within the GDPR where the UK can exercise discretion over how certain provisions are applied.
- 2.3 In September 2017, the Data Protection Bill was published setting out new standards for protecting general data in accordance with GDPR and preserving certain other exemptions of the current Data Protection Act 1998.
- 2.4 The Data Protection Act 2018 was given Royal Assent on 23 May 2018. The General Data Protection Regulation came into force on 25 May 2018 and provides an accountability-based framework for data protection in Europe.
- 2.5 In preparation for the new regulation, a GDPR work programme was developed, drawing on regional collaborative work completed with other local authorities. This was approved in July 2017 and this report provides the seventh and final quarterly update to the Cabinet (Performance Management) Panel on progress to date.

### **Progress to date and next steps**

- 2.6 The GDPR programme of work has concluded and has moved into a business as usual status. GDPR training sessions (either through briefings, face to face sessions or e-learning) were delivered to most service areas across the Council throughout the programme lifecycle and a complete review of corporate policies and procedures was undertaken. Work was carried out with many teams across the Council through the completion of a GDPR matrix document which highlighted the areas of change the new regulation introduced and identified the gaps that teams needed to address to remain compliant. Work was completed with Procurement and Legal teams to ensure third party supplier checks were introduced that would form part of the procurement process and to ensure that the Council had GDPR compliant contracts in place. New GDPR compliant template documents were also introduced, including the new statutory Data Protection Impact Assessment (DPIA) and the Council's overarching Privacy Notice and

departmental Privacy Notices. All policies and procedures and template documents will be reviewed and updated on an annual basis as part of the Information Governance team's core activities, in line with scheduled review periods.

- 2.7 Data protection compliance activities will now form part of core business activities and will be aligned with the statutory Data Protection Officer (DPO) reporting framework. This will include a review of the Information Asset Registers (IARs) that were completed and submitted by teams across the business and ensure that compliance with the new Regulation and UK Data Protection laws will be monitored and reported on an ongoing basis.
- 2.8 As part of the above, formal communications on data protection compliance will be published as and when required; either through a business need, incident or direction from the ICO.

### **3.0 Quarter four Information Governance performance reporting**

#### **Background and context**

- 3.1 The ICO has been interacting with the Council on information governance matters for several years. Considerable improvements have been made since their consensual audits in 2011 and 2012, which focused on requests for personal data (Subject Access Requests - SAR) and Freedom of Information (FOI).
- 3.2 Work has continued since the conclusion of the audit and a strategic approach to Information Governance has been adopted to ensure that the Council appropriately manages its information assets. Considerable improvements have been made in terms of processing information requests and the Council's overall statutory response rates have improved dramatically over the last five years.
- 3.3 To ensure ongoing improvements with information governance this report outlines current performance.

#### **Progress for quarter four**

- 3.4 The IG performance figures for quarter four are contained in appendix 1
- 3.5 FOI Freedom of Information and Environmental Information (FOI/EIR) – 326 requests for freedom of information and environmental information were received this quarter. This shows an increase (74) in the number of requests received since the last quarter and brings the volumes back in line with those received in the first half of the year. Three requests were responded to outside of the statutory deadline, which equates to a 99% response rate for the quarter. The response rate has remained at a consistent high this quarter and are in line with the rates reported throughout the year. The overall response rate for FOI and EIR requests for the year remains constant at 99%, as it has done for the last four years. 1247 requests were received in 2018-19, which is the highest received since 2015-16, albeit only by 92.
- 3.6 Data Protection (DP/SAR) – 88 requests for personal information were received this quarter, which is the lowest number received in all of the quarters this year. All but one request was responded to within the 30 calendar-day statutory timeframe, which brings

the response rate for quarter four to 98.9%, in line with the overall response rate for the year at 98.7%. 445 requests were received in total for the year, which is 19 fewer requests than last year. Although the volumes show a decrease from last year, it does not appear to evidence a trend as volumes have fluctuated over the last four years, albeit only by a hundred or so.

- 3.7 Information Incidents – 43 incidents were reported to the IG Team this quarter which is a slight increase from the last two quarters and brings the total of incidents reported for the year to an all-time high of 123. As mentioned in previous quarterly reports, this was expected as it was anticipated that the number of incidents reported for 2018-2019 would exceed that of previous years, due to the impact of GDPR and the new Data Protection Act and the amount of awareness raising with employees that has been carried out to prepare for the changes in law. Volumes are indicative of the fact that employees are now more aware of what constitutes a breach and of the channels to report them. All incidents reported were of the low to low/medium risk category.

#### **4.0 Evaluation of alternative options**

- 4.1 No alternative options have been considered or evaluated since this report is to provide an update on progress in terms of IG performance.

#### **5.0 Reasons for decision(s)**

- 5.1 No decisions have been presented for approval since this report is an update on progress in terms of IG performance.

#### **6.0 Financial implications**

- 6.1 There are no financial implications associated with this report as Councillors are requested to review the information governance performance figures and note the progress made on the GDPR programme of work. All work associated with delivery of training and meeting information governance requirements is covered through existing budgets.
- 6.2 It is worth noting, however, that a failure to effectively manage information governance carries a financial risk. Inaccurate and out of date information can lead to poor decision making and a potential waste of financial resources. Following the implementation of GDPR, a two-tiered sanction regime with higher financial penalties will be adopted. Lesser information incidents will be subject to a maximum fine of either €10 million or 2% of an organisation's global turnover, whichever is greater. More serious violations could result in fines of up to €20 million or 4% of turnover.  
[MH/30052019/P]

#### **7.0 Legal implications**

- 7.1 The Council has a legal duty under the current Data Protection Act 2018, GDPR 2016/679, Freedom of Information Act 2000 and Environmental Information Regulations 2004 to appropriately manage and protect information assets.

- 7.2 The integration of Public Health into the Council in April 2012 required the Council to provide assurance to the NHS that it had in place suitable Information Governance policies, procedures and processes.
- 7.3 Failure to effectively manage information governance could increase risk of exposure to fraud and malicious acts, reputational damage, an inability to recover from major incidents and potential harm to individuals or groups due to inappropriate disclosure of information.
- 7.4 The Information Commissioner has the legal authority to:
- Fine organisations for breaches of Data Protection 2018 or Privacy & Electronic Communication Regulations. With the implementation of the GDPR on 25 May 2018, a two-tiered sanction regime has been introduced and higher financial penalties will be adopted by the ICO. Lesser information incidents could be subject to a maximum fine of either €10 million or 2% of an organisation's global turnover, whichever is greater. More serious violations could result in fines of up to €20 million or 4% of turnover.
  - Conduct assessments to check organisations are complying with the Act.
  - Serve Enforcement Notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps to ensure they comply with the law.
  - Prosecute those who commit criminal offences under section 170 of the DPA 2018 (previously section 55 of the 1998 Act.)
  - Conduct audits to assess whether organisations processing of personal data follows good practice.
  - Report issues of concern to Parliament.
- 7.5 Demonstration of the Council's compliance with the current Data Protection Law protects it from legal challenges for alleged breaches of individuals' rights.  
[TS/26052019/Q]

## **8.0 Equalities implications**

- 8.1 Having considered the equalities issues presented under the new legislation - Data Protection Act 2018 and GDPR 2016/679, no new implications have been identified from associated actions or recommendations of this report.
- 8.2 Any new equalities issues that become apparent as the programme of work progresses will undergo an initial screening and if appropriate will be followed by a full equalities analysis

## **9.0 Environmental implications**

- 9.1 There are no environmental implications identified.

## **10.0 Human resources implications**

10.1 This will only be relevant for some reports but will be significant in those cases.

## **11.0 Corporate landlord implications**

11.1 There no direct corporate landlord implications identified.

## **12.0 Health and Wellbeing Implications**

12.1 There are no health and wellbeing implications identified.

## **13.0 Schedule of background papers**

13.1 Strategic Executive Board – Briefing note on GDPR – July 2017

13.2 Strategic Executive Board Report – Approach to GDPR – January 2017

## **14.0 Appendices**

14.1 Appendix 1 - Quarter four 2018-19 info-graph