

## Cabinet (Performance Management) Panel

25 June 2018

<b>Report title</b>	Information Governance Quarter Four Performance and General Data Protection Regulation (GDPR) Update Report	
<b>Decision designation</b>	AMBER	
<b>Cabinet member with lead responsibility</b>	Councillor Val Gibson Governance	
<b>Corporate Plan priority</b>	Confident Capable Council	
<b>Key decision</b>	No	
<b>In forward plan</b>	Yes	
<b>Wards affected</b>	All Wards	
<b>Accountable Director</b>	Jennifer Brake	
<b>Originating service</b>	Information Governance	
<b>Accountable employee</b>	Anna Zollino-Biscotti Tel Email	Information Governance Manager 01902 555166 Anna.zollino- biscotti@wolverhampton.gov.uk
<b>Report to be/has been considered by</b>	Corporate Directorate Leadership Team Strategic Executive Board Information Governance Board	11 June 2018 12 June 2018 21 June 2018

### Recommendations for action:

The Cabinet (Performance Management) Panel is recommended to:

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

### Recommendations for noting:

The Cabinet (Performance Management) Panel is recommended to:

3. Note that Audit Services is preparing a readiness analysis of the Council's services in relation to GDPR.

## **1.0 Purpose**

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

## **2.0 General Data Protection Regulation (GDPR)**

### **Background and context**

- 2.1 On 14 April 2016, the EU Parliament approved the General Data Protection Regulation (GDPR). The regulation came into effect on 25 May 2018 and provides an accountability-based framework for data protection in Europe.
- 2.2 In October 2016, the Government confirmed that it will implement the GDPR in the UK and that the UK's decision to leave the EU will not affect the commencement of the GDPR. The new regulations will replace the current Data Protection Act 1998 and the Information Commissioner's Office (ICO) will continue to be the supervisory authority.
- 2.3 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.
- 2.4 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. The Bill will result in a new Data Protection Act replacing the current law and will add clarity on how the UK will apply statutory controls to areas of the GDPR where Member States have been given some flexibility i.e. the derogations. As and when the UK leaves the EU the new Data Protection Act would replace the GDPR.
- 2.5 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.
- 2.6 In preparation for the new regulation, a GDPR work programme has been developed, drawing on regional collaborative work completed with other local authorities. This was approved in July 2017 and this report provides the third quarterly update to the Board on progress to date.

### **Progress of work – approach**

- 2.7 A training needs analysis (TNA) and communication plan were completed at the start of the project to identify the level of engagement required by each service area. This ranges from those who only need to be aware of the changes, as little or no personal data is processed by the service, to those who need to be actively engaged in the programme.

- 2.8 Using the information identified from the TNA, a matrix has been produced to identify those departments who are key stakeholders in GDPR work. A training priority has been assigned to each department. Appendix 1 shows the list of departments and the priority status given – 1 being high priority.
- 2.9 To ensure maximum engagement with minimum disruption, training and awareness briefings have taken place at regular team or departmental meetings. Where workshops are required, these are also being led by the IG team and comprise a pre-booked two-hour session to review areas of impact and devise service specific action plans. Progress against the plan is then monitored throughout the duration of the project, and revisited where required.

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

- 2.10 The GDPR programme of work continues and is on plan. Appendix 1 shows the service areas across the Council which have received GDPR awareness training to date, either through briefings, workshops or drop-in sessions. Most service areas that are key stakeholders and have a high training priority have received training and are now progressing individual action plans. Monitoring of these plans continues.
- 2.11 Training has also extended to support wider council relationships, with the delivery of GDPR presentations to Tenancy Management Offices (TMOs), Wolverhampton Homes, Head Teacher forums and Safer Wolverhampton Partnership Board.
- 2.12 Training has also been offered to Councillors with three training sessions held in January 2018 and a further session scheduled for 4 July 2018. Recently elected Councillors also received a GDPR overview in the Councillor induction sessions which were held on 10 May 2018. To supplement the training provided, a 66-page Councillor Information Pack was developed by the Information Governance team and has been sent to all Councillors via the Councillor Support Office. The pack provides Councillors with key GDPR compliant template documents, guidance notes and a check list of things to do to prepare for the changes and to help them to comply with the regulation, as individual Data Controllers.
- 2.13 Due to an increase in requests for training from teams during the last quarter and up to the end of May 2018, three full day drop-in sessions were provided, and nine further training sessions ran on these days. 88 employees attended these training sessions.
- 2.14 The IG Team's focus during the last quarter has been on completing corporate and service specific operational tasks. Tasks have included reviewing, updating and creating GDPR compliant policies – a new Data Protection Policy has been approved at IG Board and has been published, as has the Records Management Policy. Further IG related policies are being revised to reflect the changes (Breach Management policy and procedures and city-wide Information Sharing Protocols).

- 2.15 A new Council Privacy Notice has also been approved and published in accordance with the new requirements of the regulation. Templates have been provided to service areas for them to draft their own service specific privacy notices. These will need to be published and linked to the overarching Council privacy notice. The IG team is supporting teams with this. The data protection page on the Council website has also been updated to reflect the new regulation. As of 25 May 2018, the IG team will follow the statutory procedures for dealing with Subject Access Requests (SAR); a new standard operating procedure (SOP) is being drafted and will be finalised once guidance from the ICO has been published.
- 2.16 Work continues with Legal and Procurement to finalise the process for when statutory Data Privacy Impact Assessments (DPIAs) and Data Processing Agreements are to be used as part of the procurement process. A procedure is currently being drafted – this will also include the process for local procurement (where the procurement doesn't meet the threshold for it to be processed by the procurement team) and discussions have started with our Agresso finance business partner to identify if Agresso can provide a solution for identifying those procurements that require a DPIA.
- 2.17 The GDPR service level agreement with schools went live in April 2018 – take up has been positive (18 schools have taken up our various offerings) and work has commenced with them.
- 2.18 In line with the project's communication plan, a series of City People and Core Brief articles were published during April and May 2018. An IG team intranet portal is also being developed, however this has been delayed – as a result the team is looking to utilise the C3 portal as an interim measure to support employees on general information governance matters and particularly GDPR, and to provide links to GDPR compliant templates and forms and other supportive learning materials. In addition to the briefing sessions, the new GDPR e-learning module went live in April and will provide employees with additional guidance.
- 2.19 As part of the approved internal audit plan for 2018-2019, a health check has been started by Audit Services (May 2018) to provide assurances that the Council has the appropriate systems and controls in preparation for the implementation phase of the new regulation. A further, more detailed, audit will be scheduled in Autumn 2018 to ensure that changes have been applied and embedded across the Council.

### **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 2.
- 3.5 Freedom of Information and Environmental Information (FOI/EIR) – 317 requests were received for Freedom of Information and Environmental Information which is slightly more than last quarter (287). All but three valid requests were responded to within the statutory 20-day timeframe, which equates to a 99.05% response rate. Of the three that went over, one request was the result of an administrative error with the IG team and the other two were missed as a result of process not being followed/training need by a new member of the team. This matter has been resolved and the relevant staff member has received refresher training to limit any reoccurrence.
- 3.6 A total of 1144 FOI/EIR requests have been received for the year. This is an increase of 58 requests compared to the number of requests received last year, and more in line with the volumes received in previous years. The overall response rate for the year remains high at 99% as it has done for the last three years running.
- 3.7 Data Protection (DP/SAR) - 153 personal data requests were received this quarter which is a slight increase in volume (137) compared to the number of requests received last quarter. The response rate for this quarter has dropped slightly at 98% which may be indicative of the increase in volume and the number of complex and voluminous requests that are being received. Two requests were responded to outside of the statutory 40-day timeframe.
- 3.8 A total of 464 DP/SAR requests were received for the year. This is an increase of 113 compared to the previous year. This reflects an upward trend that is more in line with the volumes received in previous years (2015-2016) and may be indicative of the volumes we will receive in future years due to the changes the new GDPR regulation brings, specifically the removal of the £10 fee for SAR requests. The overall response rate for the year remains high at 99% echoing the response rate of the previous two years.
- 3.9 Information Incidents – the number of incidents reported for the quarter has nearly doubled; 17 incidents have been reported compared to nine reported in quarter three of this year. All incidents reported were of the low risk category. The total number of incidents reported for the year is 53, which is slightly lower than the number of incidents reported for the previous year (72); again all reported incidents have been of the low risk category.

## **4.0 Financial implications**

- 4.1 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.
- 4.2 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/06062018/L]

## **5.0 Legal implications**

- 5.1 The Council has a legal duty under the current Data Protection Act 1998 (replaced by Data Protection Act 2018 post 23 May 2018 and GDPR post 25 May 2018), Freedom of Information Act 2000 and Environmental Information Regulations 2004 to appropriately manage and protect information assets.
- 5.2 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.
- 5.3 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.
- 5.4 The Information Commissioner has the legal authority to:
- Fine organisations up to £500,000 per breach of Data Protection 1998 or Privacy & Electronic Communication Regulations. Post 25 May 2018, GDPR introduces a two-tiered sanction regime and higher financial penalties will be adopted by the ICO. 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.
  - 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 55 of the 1998 Act (and the equivalent sections in the Data Protection Act 2018 and GDPR).

- Conduct audits to assess whether organisations processing of personal data follows good practice.
- Report issues of concern to Parliament.

5.5 Demonstration of the Council's compliance with the current Data Protection Law protects it from legal challenges for alleged breaches of individuals' rights.  
[RB/06062018/B]

## **6.0 Equalities implications**

6.1 Having considered the equalities issues presented under the current Data Protection Act 1998 and new Data Protection Law (DPA 2018 and GDPR), no new implications have been identified from associated actions or recommendations of this report.

6.2 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.

## **7.0 Environmental implications**

7.1 There are no environmental implications identified

## **8.0 Human resources implications**

8.1 Working practices to support the adoption of GDPR controls and measures will be incorporated into existing Information Governance and HR policies.

## **9.0 Corporate landlord implications**

9.1 There no direct corporate landlord implications identified

## **10.0 Schedule of background papers**

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

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

## **11.0 Appendices**

11.1 Appendix 1 – GDPR Progress

11.2 Appendix 2 – Quarter four 2017-18 info graph