Report Title:	**GDPR Compliance – Progress Report**
Contains Confidential or Exempt Information?	No - Part I
Member reporting:	Councillor Rayner, Lead Member for Resident and Leisure Services, HR, IT, Legal, Performance Management and Windsor
Meeting and Date:	Corporate Overview and Scrutiny Panel 18 November 2019
Responsible Officer(s):	Karen Shepherd, Head of Governance
Wards affected:	All

www.rbwm.gov.uk
Royal Borough of Windsor & Maidenhead

REPORT SUMMARY

1. The Corporate Overview and Scrutiny Panel reviewed the 2018/19 Annual Governance Statement (AGS) on 30 July 2019. Although formal approval of the AGS was deferred to a later meeting, the Panel requested that update reports on issues identified in the accompanying Action Plan be presented to the Panel at appropriate future meetings.

2. General Data Protection Regulation (GDPR) compliance was identified in the AGS as an area for improvement, with a timescale for actions to be taken of October 2019. This report therefore provides an update on actions undertaken since spring 2019 when Heads of Service completed Management Assurance Statements identifying GDPR compliance as an area of concern, and proposed future actions to continue to improve GDPR compliance across the council.

1. DETAILS OF RECOMMENDATION(S)

RECOMMENDATION: That Corporate Overview and Scrutiny Panel notes both actions already taken and those planned to further improve GDPR compliance across the council.

2. BACKGROUND

2.1 The Annual Governance statement for 2018/19 identified GDPR compliance as a corporate issue and was therefore included in the AGS Action Plan (see extract at Appendix A).

3. PROGRESS TO DATE TO ADDRESS ACTIONS IDENTIFIED IN THE ANNUAL GOVERNANCE STATEMENT

3.1 The Electoral and Information Governance Services Manager (Suzanne Martin) undertook training in July 2019 to become a certified Data Protection practitioner. Following successful completion of the training and examination, Suzanne was appointed as Deputy Data Protection Officer on 4 September 2019. Suzanne supports the work of Jennifer Shaw, the Data Protection Officer (DPO).

3.2 The council's induction programme for new employees includes mandatory training on data protection. Additionally, all staff are required to undertake annual refresher training. This ensures over 90% staff are fully trained in data protection and data management at all times.

3.3 The DPO attended Member Induction sessions in May 2019 to provide guidance to both new and returning Members on their data protection obligations and a Member FAQ sheet is available on the Members' Hub. Online training has also been made available for Members of the council and promoted to parish clerks and councillors.

3.4 The DPO regularly liaises with the Senior Information Risk Owner (SIRO) and members of the Corporate Leadership Team to inform them of breaches that have occurred, mitigation actions and lessons learned.

3.5 The DPO regularly promotes data protection awareness via all-employee emails and Borough Bulletin articles. The latest all-employee email (see appendix B) highlighted recent Information Commissioners Office (ICO) prosecutions of misuse of data and reminded employees of their responsibility to access data only when they have a business need to do so. The DPO regularly issues Borough Bulletin updates when breaches have occurred in other authorities that would be relevant to our organisation.

3.6 To date over 100 privacy notices have been published to the council website to portray the information journey of personal data processing relevant for each purpose within services. Work is underway to review the privacy notices published since May 2018 to improve the council's compliance with the transparency principle applicable to the GDPR.

3.7 Significant work has been undertaken to assist Members with constructing their own privacy notices as individual data controllers. Members have been provided with a privacy notice template which can be tailored to their specific requirements. As of 7 November 2019, 17 councillor privacy notices have been published on the website; efforts will continue to support and encourage all councillors to complete their privacy notices.

3.8 Since the transfer of the delivery of children's and adult services to partner organisations (Achieving for Children (AfC) and Optalis respectively) responsibility for data protection compliance in respect of these services has also transferred to the partner organisation who are data controllers in their own right. Through the monthly commissioning meetings, the council's DPO is informed when data breaches occur. Information Sharing Agreements (ISAs) between the council and each of its partner organisations are required as part of partnership working, where personal data is shared. ISAs are in place with both Optalis and AfC.

4. PLANNED ACTIONS

4.1 Earlier in 2019, all Heads of Service were requested to identify a Data Protection link officer to liaise with the Data Protection Officer (DPO). Following the senior management restructure that took effect on 1 October 2019, the list of identified officers is under review to ensure all services are covered. Once finalised, a meeting between the DPO and link officers will be arranged to set out the

responsibilities of link officers and areas for immediate action. The initial focus will be on reviewing privacy notices already published and updating the service area Information Asset Registers. A second phase will focus on updating service area Record of Processing Activity Registers (RoPA).

4.2 The council's DPO also acts as the DPO for 36 of the borough's schools. This arrangement is currently via formal contracts where the DPO's services are charged at £95 per hour or part thereof. Unfortunately this arrangement has proven inefficient as it is difficult for the DPO to track time spent on schools as work is mostly slotted in between other priorities. Additionally, where significant time is required as a result of a data breach or complex subject access request, the charging rate is unfeasible for schools. It has therefore been decided to move to an alternative format and offer DPO services to schools as part of the traded service agreement. The Director of Children's Services has been consulted and officers are developing a sliding scale charge rate. It is therefore intended that the DPO will then be available to schools as a flat fee service. This will ensure schools can include the cost when setting their budgets and encourage schools to work with the DPO on a regular basis, improving oversight.

4.3 The council's Data Protection service is currently the subject of an internal audit review, in accordance with the 2019-20 Annual Internal Audit Plan agreed by Members. The principal objective is to determine whether controls in place for data protection and GDPR compliance in relation to entries FOI0003 / 06 in the Corporate Risk Register are operating effectively, and that risks are minimised through proper and adequate control measures. The final report is expected in December 2019. All recommendations will be reviewed and actioned as appropriate in conjunction with the proposals in paragraphs 4.1-4.2 above.

5. FINANCIAL DETAILS / VALUE FOR MONEY

5.1 There are no financial implications as a result of the recommendation in this report.

6. LEGAL IMPLICATIONS

6.1 The council is required to comply with both the UK Data Protection Act 2018 and the General Data Protection Regulation (GDPR) 2016. The Information Commissioner's Office (ICO) is the UK's supervisory authority which monitors and regulates data protection compliance. The ICO has powers of enforcement and can issue a monetary penalty to data controllers and processors in the event that data protection legislation has been breached. The GDPR allows the ICO to issue a maximum fine of up to 20 million euros or 4% of annual turnover (whichever is the higher) to a data controller where a serious data protection breach has occurred. The effect of a breach of data protection legislation which results in a fine issued by the ICO may have serious repercussions on the financial integrity of the council and would lead to reputational damage.

7. RISK MANAGEMENT

7.1

Table 1: Impact of risk and mitigation

Risks	Uncontrolled risk	Controls	Controlled risk
Failure to comply with the UK Data Protection Act 2018 and the General Data Protection Regulation 2016	High	Maintain Record of Processing Activity Register (RoPa) Maintain Information Asset Register (IAR) Produce and regularly review information sharing agreements (ISA) between the council and third parties Ensure data protection impact assessments are undertaken where required Ensure services publish privacy notices for all purposes of personal data processing Promote personal data concern/breach reporting process Maintain data breach spreadsheet incorporating remedial actions and review timelines to ensure these are embedded in service areas Ensure all new employees are required to complete data protection e-learning and all employees undertake annual refresher training Targeted training and guidance provided to Members on their data protection obligations	Low

Risks	Uncontrolled risk	Controls	Controlled risk
		Targeted and tailored data protection training delivered to services where a personal data processing concern or breach has been reported. Regular news and articles in Borough Bulletin regarding data protection issues to ensure employee awareness of data protection obligations is maintained	

8. POTENTIAL IMPACTS

8.1 Equalities. No impacts identified

8.2 Climate change/sustainability. No impacts identified

8.3 Data Protection/GDPR. Impacts detailed throughout the report

9. APPENDICES

9.1 This report is supported by two appendices:

- Appendix A - Extract from the Annual Governance Statement Action Plan
- Appendix B – Email sent to all RBWM employees 17/10/19

10. BACKGROUND DOCUMENTS

10.1 This report is supported by one background document:

- The RBWM Annual Governance Statement 2018/19

11. CONSULTATION (MANDATORY)

Name of consultee	Post held	Date sent	Date returned
Cllr Rayner	Lead Member for Resident and Leisure Services, HR, IT, Legal, Performance Management and Windsor	5/11/19	7/11/19
Duncan Sharkey	Managing Director	1/11/19	4/11/19
Russell O'Keefe	Executive Director	1/11/19	

Name of consultee	Post held	Date sent	Date returned
Andy Jeffs	Executive Director	1/11/19	
Terry Neaves	Interim S151 officer	1/11/19	
Elaine Browne	Head of Law	1/11/19	
Mary Severin	Monitoring Officer	1/11/19	4/11/19
Nikki Craig	Head of HR, Corporate Projects and ICT and Senior Information Risk Owner (SIRO)	1/11/19	4/11/19
Louisa Dean	Communications	1/11/19	7/11/19
Kevin McDaniel	Director of Children's Services	1/11/19	1/11/19
Hilary Hall	Director Adults, Commissioning and Health	1/11/19	4/11/19

REPORT HISTORY

Decision type: For information	**Urgency item?** No	**To Follow item?** No
Report Authors: Jennifer Shaw, Data Protection Officer, 01628 796675 and Suzanne Martin, Deputy Data Protection Officer, 01628 682935		

Appendix A

Extract from Annual Governance Statement 2018/19 Action Plan

	Area for Improvement	**Actions**	**Owner**	**Timescale**	**Improvement outcome**
AGS 19.4	GDPR Compliance. There is a lack of clarity in respect of data ownership and information governance procedures.	1. Ensure all staff are fully trained in data protection and data management. 2. Ensure that there are regular liaison meetings the Data Protection link Officers and the Council's Data Protection Officer 3. DPO to provide regular briefings to CLT in respect of breaches 4. Deputy DPO to become certified practitioner to provide resilience	DPO	October 2019	Reduction in breaches Clarity in respect of data ownership and procedures

Email sent to all RBWM employees 17/10/19

Data protection reminder – accessing personal information via borough systems

Many of us will have access to internal systems in the borough that contain information or personal data about the residents we provide services to and the employees who work here. It is our responsibility to ensure that the information we access on a daily basis is used strictly for the purposes of fulfilling the requirements of our roles in the services which we operate. Accessing records where you have no business requirement to do so may be a criminal offence.

All employees are required to complete mandatory data protection/GDPR e-training as part of their induction followed by an annual refresher course. Adherence to data protection obligations is critical not only for the benefit of employees but also for our residents whose information we are custodians of. Any breach or concern regarding data protection compliance is investigated by our data protection officer, Jennifer Shaw. In cases where we believe records may have been accessed without a business need, audits to systems/records will be undertaken which may lead to disciplinary measures and ultimately dismissal.

The borough has had several incidents in recent years where employees have inappropriately accessed records. The individuals involved no longer work with us.

Around the UK, prosecutions have been made by the Information Commissioner's Office when individuals have failed to follow the correct guidelines:

26 February 2019 – prosecution for a senior government officer who shared personal information from job applicants with their partner

A former senior local government officer has been prosecuted for passing the personal information of rival job applicants to his partner who had applied for a job at the council. Kevin Bunsell accessed the authority's recruitment system and emailed the personal information of nine rival shortlisted candidates to his partner's Hotmail account. The recruitment packs included the name, address, telephone number and CV of each candidate. Mr Bunsell of Bedworth appeared before Nuneaton Magistrates' Court and admitted an offence of unlawfully sharing personal data, in breach of s55 of the Data Protection Act 1998. He was fined £660, ordered to pay costs of £713.75 and a victim surcharge of £66.

7 June 2019 – prosecution for a customer service advisor accessing records without authorisation

A former customer service advisor at Stockport Homes has been prosecuted for accessing records relating to anti-social behaviour without authorisation. An internal investigation found that Wendy Masterson had inappropriately accessed cases without any business reason to do so. The records related to victims, witnesses and perpetrators of anti-social behaviour. Ms Masterson of Stockport appeared before Stockport Magistrates' Court and pleaded guilty to the offence of unlawfully obtaining personal data, in breach of s55 of the Data Protection Act 1998. She was fined £300, ordered to pay £364.08 costs and a victim surcharge of £30.

If you have any queries regarding data protection concerns/breaches or whether accessing records or systems is appropriate in a particular scenario please speak to your line manager or contact our data protection officer, Jennifer Shaw on 01628 796675 or by email dpa@rbwm.gov.uk.

Message to all employees in Borough Bulletin 31/10/19

Message from the data protection officer:

West Berkshire Council recently suffered a data breach where 1,107 residents were contacted via email to complete a leisure survey. Unfortunately, the email was not sent using blind copy, and all of the recipients were able to see the other email addresses.

Please be sure to double check that blind copy is used in such instances that a group email is sent to personal email addresses.

Although West Berkshire's incident has a low level of harm, it could have been much more severe if the email contained personal information rather than a leisure survey.