

**Agenda Item No:** 4  
**Report To:** AUDIT COMMITTEE  
**Date:** 6 December 2016  
**Report Title:** DATA PROTECTION UPDATE  
**Report Author:** Rich Clarke



**Summary:** The report sets out progress made since this Committee received the 'weak' assurance review of Data Protection.

Although this report does not record a change to the assurance level, it documents further progress. Steps taken include appointing specialist consultants to bring forward policy and procedure development to enable the Council to address recommendations ahead of substantive appointment of the new Data Protection Officer. .

**Key Decision:** No

**Affected Wards:** All

**Recommendations:** **1. The Audit Committee NOTES the progress made towards implementing recommendations raised in the Data Protection Audit Report brought to this Committee in March 2016.**

**Policy Overview:** Not Applicable

**Financial Implications:** Not Applicable

**Risk Assessment** No

**EIA** No

**Other Implications:** Not Applicable

**Exemptions :**

**Background Papers:** Data Protection Audit Report (presented March 2016)  
Data Protection Update (presented September 2016)

**Contacts:** rich.clarke@midkent.gov.uk – Tel: (01233) 330442

## Report Title: Data Protection Update Report

### Purpose of the Report

1. This report follows up from an update presented to Members in September 2016 and describes progress towards implementing recommendations to address a 'weak' audit report finding from earlier this year.
2. For Members convenience, we repeat the background in paragraph 3 from our September report. New information on progress begins at paragraph 4.

### Background

3. The audit report, dated 26 February 2016, was reported to Members in March 2016. For context and a summary of the findings, we reproduce below the original executive summary:

*The council has documented policies and procedures, also allocated roles and responsibilities, however there are weaknesses as policies are not operated (the monitoring checks) as described and there are no deputy arrangements to provide formal cover in the Data Protection Officer's absence. The Data Protection function is currently subject to staff changes and consideration of future service delivery and resource arrangements.*

*The Data Protection Policy makes clear commitments on training provision and we found that guidance was available to staff, however training and awareness arrangements are less well established. There is no mandatory post induction refresher requirement, no formal records to evidence training for key staff (such as the Data Protection Officer) and only 58 staff evidenced as having completed the E Learning package.*

*Compliance with Data Protection requirements is not monitored by the council (the review processes noted in policy and job descriptions) as provided for in key documents. Interviews with various services identified some services with better understanding and application of data protection requirements (such as the Monitoring Centre and Fraud Investigations). We found the Council's Members Allowance IT Scheme required recipients to register, however only 5/23 were registered. We found that there were no central logs to record statistics and help reporting (Subject Access Requests and Breach Notifications or near misses).*

*Staff advised that no breaches had been reported to the Information Commissioner. Arising from the absence of an incident / referral log it was not possible to assess the number or nature of any internal referrals made. In addition, the access capability to records is limited to the Data Protection Officer as material is held in E records (personal email and e filing) rather than generic E records to enable authorised deputy access.*

4. The table below summarises the position to date on implementing recommendations. We provide further detail and commentary below. We have not included recommendation 8 (on fee handling) as we were satisfied that had been implemented on time

Recommendation Priority Rating Original implementation date	Finding at September 2016 (as reported to Members)	Finding at November 2016
<p><b>R5: Training</b></p> <p><i>Implement training regime and awareness programme</i></p> <p>Priority 2: <b>High</b> Implementation: April 2016</p>	<p><b>Partly implemented.</b></p> <p><b>General training</b> underway and delivered to 91% staff.</p> <p><b>Specific training:</b> For key officers, scheduled mid-October</p>	<p><b>Implemented</b></p> <p>Specific training has now been delivered for key staff.</p>
<p><b>R6: Breach Handling</b></p> <p><i>Formalise and enhance protocols for breach handling</i></p> <p>Priority 2: <b>High</b> Implementation: July 2016</p>	<p><b>Partly implemented</b></p> <p>The new data protection policy sets out what should be done in case of breach. Revised protocols will be established by the DPO when appointed. Currently, legal services are handling instances case-by-case.</p>	<p><b>Implementation to be verified</b></p> <p>Specialist Consultant appointed to accelerate progress on key steps ahead of DPO appointment. Will report in December 2016 on new procedures.</p> <p>The procedures have been used in practice on recent minor breaches. Management are satisfied procedures have operated effectively; we will verify through testing as part of our next follow up round in January 2017.</p>

<b>Recommendation</b> <b>Priority Rating</b> <b>Original implementation date</b>	<b>Finding at September 2016</b> <b>(as reported to Members)</b>	<b>Finding at November 2016</b>
<p><b>R1: Policy &amp; Procedure</b></p> <p><i>Update and apply policies and procedures</i></p> <p>Priority 3: <b>Medium</b> Implementation: June 2016</p>	<p><b>Partly implemented</b></p> <p>The new policy was agreed by Cabinet on 14 July 2016.</p> <p>There is some expanded guidance available on the intranet that will be revised and extended by the DPO.</p>	<p><b>Partly implemented</b></p> <p>The specialist consultant’s brief includes reviewing/updating the policy base to reflect current best practice in advance of DPO appointment. This includes breach management, “top – tip” guidance to staff, and Subject Access Request (SAR) and data sharing policies.</p> <p>Revised implementation January 2017.</p>
<p><b>R2: Organisational Monitoring &amp; Review</b></p> <p><i>Implement monitoring and review regime</i></p> <p>Priority 3: <b>Medium</b> Implementation: June 2016</p>	<p><b>Not implemented</b></p> <p>Reporting framework will be developed by the DPO when appointed. In the meantime, legal services will have awareness of compliance with DPA requirements.</p>	<p><b>Partly implemented</b></p> <p>The policy base is currently under review by specialist consultants who are also preparing compliance monitoring protocol for provide practical guidance. Full roll out will be for the new DPO, interim measures have been taken, including, completion of further training, and a DPA “champion” update report to Management Team on breach handling and other DP matters. So some monitoring and review activity is in place already.</p> <p>Revised implementation: In full, March 2017</p>

<b>Recommendation Priority Rating Original implementation date</b>	<b>Finding at September 2016 (as reported to Members)</b>	<b>Finding at November 2016</b>
<p><b>R9: Record Handling</b></p> <p><i>Review and revise arrangements for data storage and retention to ensure compliance with retention requirements.</i></p> <p>Priority 3: <b>Medium</b> Implementation: June 2016</p>	<p><b>Not implemented</b></p> <p>Initial email review undertaken. A timetable of the steps for ensuring compliance is due before management team in November.</p>	<p><b>Not implemented</b></p> <p>Considered further by management team in November. Detailed retention and handling policy now a corporate project – see para 6 below</p> <p>Revised implementation date August 2017</p>
<p><b>R3 Roles &amp; Responsibilities</b></p> <p><i>Revise job descriptions and supporting arrangements (Deputy and Back Up arrangements)</i></p> <p>Priority 3: <b>Medium</b> Implementation: July 2016</p>	<p>Not part of follow up exercise in this round.</p>	<p><b>Implemented</b></p> <p>Roles and responsibilities clarified in part through creation and approval of DPO job description.</p> <p>The current policy makes it clear that the Chief Executive is ultimately responsible for ensuring information is appropriately protected and that the DPA is complied with.</p>

<b>Recommendation Priority Rating Original implementation date</b>	<b>Finding at September 2016 (as reported to Members)</b>	<b>Finding at November 2016</b>
<p><b>R4: Shared Access</b></p> <p><i>Records accessible to a minimum of 2 authorised staff</i></p> <p>Priority 3: <b>Medium</b> Implementation: July 2016</p>	<p>Not part of follow up exercise in this round.</p>	<p><b>Implemented</b></p> <p>Records are accessible via a shared drive.</p>
<p><b>R7: Centralised Records</b></p> <p><i>Devise and maintain central records / logs of Subject Access Requests and Breaches (potential and notifications)</i></p> <p>Priority 3: <b>Medium</b> Implementation: July 2016</p>	<p>Not part of follow up exercise in this round.</p>	<p><b>Implemented</b></p> <p>Records are accessible via a shared drive.</p>

5. Much of previous discussion around recommendations centred on the creation and filling of the new post of Data Protection Officer. We understand that final interviews for that post are due to take place in early December. This appointment aims to assist longer-term compliance and monitoring strategies. However since autumn management have given added urgency and impetus to full implementation of the recommendations. Specialist consultants have been appointed with a wide-ranging brief to bring forward policy and procedure work to ensure recommendations can be met sooner than would otherwise have been possible. The likely timescales are now reflected in the table above. On this basis management are confident that the assurance rating should move up by the time of the next update report.
6. Recommendation 9 (Record Handling) has a longer implementation date to August 2017. Based on our experience, an effective data retention policy takes some time to compile. A common pitfall is to transfer a policy from elsewhere as a quick fix only to find that it is either overly bureaucratic and burdensome in its detail, or not well suited to the organisation's business and practices. For such a policy to be effective, we recognise the value in taking time in carefully considering the needs of the organisation and so are satisfied that August 2017 represents a reasonable timescale. In the meantime, the legal service will continue to offer advice and guidance on retention and handling of key documents.

## **Risk Assessment**

7. This report is presented for information and update. It has no fresh risk management implications.

## **Equalities Impact Assessment**

8. There are no proposals made in the report that require an equalities impact assessment.

## **Other Options Considered**

9. Not applicable

## **Consultation**

10. An earlier version of this report was presented to management team in mid-November. .

## **Implications Assessment**

11. Not Applicable

## **Handling**

12. Not Applicable

## **Conclusion**

13. The Council is making further substantive progress on meeting the recommendations including speeding up implementation through appointing a specialist consultant. The progress on appointment of the Data Protection Officer aims to ensure longer-term compliance and monitoring procedures will be embedded. We will continue to follow up recommendations as they fall due and note management's expectation of being able to report on a higher level of assurance in our next follow up report to management, due in February/March 2017.

## **Portfolio Holder's Views**

14. We understand the portfolio holder has been kept informed of progress in implementing recommendations.

**Contact:** Rich Clarke Tel: (01233) 330442

**Email:** [richard.clarke@ashford.gov.uk](mailto:richard.clarke@ashford.gov.uk) or [rich.clarke@midkent.gov.uk](mailto:rich.clarke@midkent.gov.uk)



