Agenda Item No:	4
Report To:	AUDIT COMMITTEE
Date:	29 September 2016
Report Title:	DATA PROTECTION UPDATE
Report Author:	Rich Clarke

ASHFORD
BOROUGH COUNCIL

Summary:	The report sets out progress made since this Committee received the 'weak' assurance review of Data Protection. The report notes that the assurance level remains 'weak' as re-considered by audit this month owing to limited practical progress on implementing recommendations, including high priority matters with an agreed target date of June 2016. Although some interim measures are in place, many of the recommendations still require a long term solution.

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

Report Title: Data Protection Update Report

Purpose of the Report

1. Our audit plan, approved by Members in March 2015, included an audit intended to examine the controls designed and operated by the Council to ensure it meets its obligations under legislation and regulations on Data Protection. That report concluded the controls offered only *weak* assurance, meaning the service required support to operate consistently at an effective level.

2. The audit included nine recommendations for improvement, all accepted by management who proposed target dates for implementation across June and July 2016. The majority of recommendations (6/9, including both high priority matters) fell due at the end of June and so we re-examined and tested for implementation as part of our quarter one 2016/17 follow-up work.

Background

3. The audit report, dated 26 February 2016, was reported to Members in March 2016. We undertook the fieldwork it reported between October and December 2015 and the final report including management comments followed a draft presented on 11 January 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 that 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 facilitate 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. Nine of the ten recommendations made had a priority rating and formed part of our follow up exercise. A tenth recommendation, relating to a reporting process improvement, we rated as advisory so it not part of our follow up. Six of the nine recommendations had an implementation date falling before 30 June 2016 so were assessed as part of our follow-up exercise, although to inform our future work programming we also sought information on progress against the three not yet due.

5. At this stage it is important to note that implementation dates are agreed in a discussion between audit and management rather than imposed by audit. Our standard approach includes suggestions for implementation timescales (for instance, a medium priority report within the next six months to a year) but we recognise each action must be assessed on its specifics and so regularly vary from that guideline. This is mostly for practical reasons, although the risk facing the authority by continuing non-implementation is also a factor. Where a recommendation will take a long time to implement – for example if the authority decides to address the issue with a new appointment – we would expect to see interim measures in place to mitigate the risk until a permanent resolution is in place.

6. For instance, we reported similar conclusions on Data Protection at Tunbridge Wells in late 2015 and updated Members there on progress in March (link). There, key recommendations had not been implemented as planned but we detailed actions – such as an increased profile of the Senior Information Risk Officer and all-staff briefings – in place to keep issues visible and lower the risk of breach.

7. On the Ashford BC follow up, the table below describes our findings against each recommendation (including those not yet due).

Recommendation	Finding
R5: Training *Implement training regime and awareness programme* Priority 2: High Implementation: April 2016	Partly implemented. **General training** available through eLearning and has been publicised to staff. Up to 5 September, this training was complete by 91% of staff.

Recommendation	Finding
	Specific training: Officers are currently drawing up information on which services require additional training because of the data they handle (e.g. Housing). A brief, funding and content for the training is agreed and arranged for delivery in mid October. We will follow up on delivery of this training later in the year.
R6: Breach Handling *Formalise and enhance protocols for breach handling* Priority 2: High Implementation: July 2016	Partly implemented. The new data protection policy sets out what should be done in base of breach. Revised protocols will be established by the DPO when appointed. Currently, legal services are handling instances case-by-case.
R1: Policy & Procedure *Update and apply policies and procedures* Priority 3: Medium Implementation: June 2016	Partly implemented The new policy was agreed by Cabinet on 14 July 2016. There is some expanded guidance available on the intranet that will be revised and extended by the DPO.
R2: Organisational Monitoring & Review *Implement monitoring and review regime in line with policy* Priority 3: Medium Implementation: June 2016	Not implemented Reporting framework will be developed by the DPO when appointed. In the meantime, legal services will have awareness of compliance with DPA requirements.
R9: Record Handling *Review and revise arrangements for data storage and retention to ensure compliance with data protection record retention requirements.* Priority 3: Medium Implementation: June 2016	Not implemented Officers undertook an initial review as part of the email archive solution and established that this is a much more substantial task than originally anticipated. The next major step for reviewing arrangements will be taken in November. A timetable of the steps for ensuring compliance is due before management team in November.

Recommendation	Finding
R8: Fee Handling *Formalise fee handling and baking arrangements for SARs* Priority 4: Low Implementation: June 2016	Implemented. Guidance has been published on the intranet stating that the fee is required and how it should be banked. We also note that, when the forthcoming General Data Protection Regulations are implemented over the next two years, this point will become moot.

8. Recommendations 3 (on roles and responsibilities), 4 and 7 (on ensuring shared access to information to help functional resilience) were not due for follow up in this period. However, in both instances we noted some progress. On R3 this was principally in the form of agreeing a job description and specification for a Data Protection Officer. On R4 and R7, subject access requests information is now held centrally within legal's case management system pending transfer to the Data Protection Officer. Development of a permanent detailed protocol on breach handling and recording will be prepared by the DPO, including arrangements for shared access. In the meantime a shared interim record system has been created in the legal services case management system.

9. In summary, although we acknowledge some areas of strong progress – most notably on general training and awareness raising – However full implementation of some recommendations is dependent on the DPO appointment. In the meantime resources have therefore been focussed on controlling operational risk, but officers acknowledge that this can only be a short term solution owing to the strain it places on existing resources.

10. We also note that during the period since March, the Council has noted no actual or potential breaches of its DPA requirements. Consequently we were unable to test whether these interim arrangements would be effective in handling a breach.

11. There is, however, insufficient progress to consider revising the assurance level from 'weak'. Officers have suggested initially moving implementation dates to the end of September 2016 but given how much progress is awaiting the Data Protection Officer (who will inevitably take some time to settle into the role) we believe full implementation before the end of 2016/17 is unlikely.

12. Therefore we encourage officers to consider extending its interim measures, potentially with further support, until a longer term solution is identified. To that end, we have put Ashford officers in contact with colleagues at Tunbridge Wells to discuss, among other considerations, whether there is scope for learning from their experience and responses they have developed to similar recommendations.

Risk Assessment

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

Equalities Impact Assessment

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

Other Options Considered

15. Not applicable

Consultation

16. An earlier version of this report was presented to management team in mid-September. This version is updated for comments received.

Implications Assessment

17. Not Applicable

Handling

18. Not Applicable

Conclusion

19. Progress to date against recommendations raised within the *weak* rated audit of data protection has not been as rapid as suggested by management in response to the audit recommendations. Although interim measures are in place to mitigate key risks, the Council must seek a longer term solution to ensure it can meet DPA requirements.

Portfolio Holder's Views

20. 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 or rich.clarke@midkent.gov.uk