APPENDIX 4

AUDIT REPORTS WITH MODERATE OR LOW LEVEL OF ASSURANCE ISSUED QUARTER 1 2018/19

IT Governance: The Council's Compliance with General Data Protection Regulations – Follow-up – 22 May 2018

1 **Introduction**

1.1 In accordance with the Audit Plan for 2018/19 a follow up review (of the 2017/18 audit review of the forthcoming General Data Protection Regulations – GDPR) changes has been completed. This report presents the updated position and the findings and conclusions drawn from the audit for information and action where appropriate.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and co-operation received during the audit.

1.3 The previous report and accompanying action plan is included at Appendix B for information. (See online version of report included as part of Committee Agenda.)

2 **Background**

2.1 The purpose of the audit was to obtain an updated position on the previous review and also gauge the state of preparedness for the forthcoming changes to the General Data Protection Regulations, due in May 2018.

3 **Scope and Objectives of the Audit**

3.1 This was an assurance review of the information governance arrangement in light of the legislation changes in May 2018 with the scope and objectives being the same as previously, but with an updated position.

4 **Findings**

4.1 **Recommendations from Previous Report**

4.1.1 The current position in respect of the recommendations from the audit reported in March 2018 is as follows:

	Recommendation	Management Response	Current Status
1	A programme of targeted awareness raising events (workshops, short training courses / sessions, etc.) and updated communications for Council staff should be introduced at an early point once the new person is in post.	An awareness briefing session is being designed for roll out via meta compliance to go out in in March.	Completed: A Councillor training session took place which was attended by 36 of the 46 Councillors. The remaining ten are being given additional opportunities to receive the training. Meta Training (MT) software has been purchased which needs Active Directory accounts to be linked with the cloud provider of MT. The first MT will be for SMT, the Democratic Services Manager, the ICT Services Manager and the Assets Manager. A briefing aimed at Information Asset Owners (IAOs) has also been done. Other staff will then be targeted. The MT training programme is also being developed.
2	A full review of all relevant policies and procedures should take place once the new officer is in post.	A report is being brought to Executive in April seeking approval of the Information Governance Framework and associated high level polices. This will also set up the framework for approval of relevant guidance.	Completed: The overall high level framework is now developed and the strand below this is also in place. The 'third level' is drafted and requires approval of SMT (planned for 23 May 2018). Note: Data Retention & schedule one is requiring a full review and is planned.

3 An information audit should be undertaken and Information Asset Owners should be appointed (and trained as appropriate) as soon as practical.	The Information Audit is underway with returns being received from Service Areas. Heads of Services are the Information Asset Owners this is being embedded in new Information Governance Policies. Training sessions are being provided as required along with a pre-briefing before the role out of each audit.	Completed: IAOs are identified in the new policies and framework.
4 The Council should document and implement a procedure for Data Protection Impact Assessments (DPIA).	This document is in draft form ready to go through the approval process.	Partially Implemented: Some service areas have started to write these with guidance from the Information Governance Manager (IGM). The IGM is meeting with teams to help with the process and is keeping a checklist of progress. (See 4.2.1 below for the view of a sample of the staff responsible).
5 A comprehensive information audit should be undertaken to formulate an Information Asset Register sufficient to meet the requirements of Article 30.	The Information Audit is underway with returns being received from Service Areas. (20 out of 24 teams have started, four are nearly completed) Progress is being monitored and teams are being actively supported with the audit.	Partially Implemented: Some areas have still to complete this. The IGM has taken / is taking this up with Heads of Service. (See 4.2.1 below for the view of a sample of the staff responsible).
6 The Council should review and / or introduce compliant information sharing agreements.	Information sharing with partner agencies is being identified through the information audit, and via a review of third party and contract arrangements. There will be an action plan for each agreement where non-compliance is identified.	Completed: A guidance email has been produced and all contractors and partners have been written to. The IGM is keeping a monitoring sheet.

4.1.2 In order to allow for progress on the incomplete actions to be further tracked, they have been included again in the action plan.

4.2 Additional Work

4.2.1 During the audit, the opportunity was taken to extend the testing of the degree of awareness of those staff (essentially Information Asset Owners etc.) who will be required to undertake specific tasks in order to become compliant. The results of these discussions revealed that there was still a considerable degree of uncertainty as to what the changes mean to them in terms specific to them and their information management responsibilities. Based on the discussions held, there is a sense within the staff-base who are directly impacted by the changes that they are being provided with general advice and guidance, but not yet anything specific to their prevailing circumstances, and consequently are still unsure of the real impact to them and the work they must now do.

Risk

Staff responsible for implementing the changes may not be fully-conversant with their obligations or specific responsibilities or tasks, which could result in varying degrees of application of the legislation.

Recommendation

The new Information Governance Manager moves to working directly with the Information Asset Owners to guide them individually on their requirements, rather than issuing generic advice and guidance.

5 Conclusion

5.1 Progress on implementation of the agreed actions has been good with four out of six being fully implemented and two partially implemented. Progress had been made on the review of policies and procedures, the information governance structure, information sharing agreements, awareness-raising, and identification of asset owners. Work is ongoing on the Data Protection Impact Assessments, and the information audit. This would indicate that the assurance can now be upgraded to MODERATE. (It had previously been awarded a 'Limited' Level of Assurance.)

5.2 The assurance bands are shown below:

Level of Assurance	Definition
Substantial Assurance	There is a sound system of control in place and compliance with the key controls.
Moderate Assurance	Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls.
Limited Assurance	The system of control is generally weak and there is non-compliance with controls that do exist.

5.3 The actions in the previous review concentrated on the corporate activities such as policies and procedures, key documentation, such as information asset registers, and user awareness-raising. As part of this follow up review, conversations were held with users who are asset owners and who will need to know what GDPR means to them in detailed and specific terms. The results of these discussions highlighted that there was still a high degree of uncertainty about the specific actions and tasks that need to be undertaken in order to become compliant. Advice, it was felt thus far, had been quite generic and not specific to any one service area or individual. An example was whether or not privacy notices are required and if so, what information and to what level of detail is required.

6 Management Action

6.1 The recommendations arising above are reproduced in the Action Plan for management attention.