APPENDIX 3 – Executive Summaries finalised since last update to Accounts, Audit & Risk Committee September 2021

GDPR 2021/22

Overall conclusion on the system of internal control being maintained	A

RISK AREAS	AREA CONCLUSION	No of Priority 1 Management Actions	No of Priority 2 Management Actions
Corporate Policy	R	0	1
Governance Structure	R	1	1
Information Audit	R	1	0
Privacy Notice	A	0	2
Data Subject Rights	G	0	0
Data Breaches	A	0	1
Privacy by Design	A	0	2
		2	7

Opinion: Amber	
Total: 9	Priority 1 = 2 Priority 2 = 7
Current Status:	
Implemented	0
Due not yet actioned	0
Partially complete	0
Not yet Due	9

The UK GDPR (General Data Protection Regulation) 2021 and the Data Protection Act 2018 collectively set out the UK's data protection regime. The UK GDPR incorporates the EU GDPR regulation into UK law, following withdrawal from the European Union.

We have identified several control weaknesses which pose a risk in terms of data protection compliance. There is no formally documented corporate policy setting out the organisation's approach to meeting its data protection obligations and there is an outstanding management action, from the previous audit on GDPR in 2018/19, to put in place a data retention policy to comply with the storage limitation requirement of GDPR. These are key policies required to support the organisation's data protection compliance regime. The Council has a current data protection registration which expires in March 2022.

The Data Protection Officer (DPO) role, which is mandatory for all public authority's, is shared with OCC and performed by the Information Services Manager. There are no further defined roles and responsibilities for data protection at the Council and thus no ownership of compliance obligations at a service level to support the DPO. CDC require all staff to undertake annual training on data protection and there is a course for staff which has an 85% completion rate and another for managers which has a 70% completion rate. Improvement to the completion rate for both courses would help ensure staff are fully aware of their data protection responsibilities.

One of the key changes introduced by GDPR is the requirement to maintain records of all processing activities, which is important as it supports good data governance and helps demonstrate compliance with UK GDPR. Information Asset Registers have recently been developed as records of processing activities, but we found they are incomplete and do not capture all relevant details.

Privacy notices need to be improved to ensure the individual's right to be informed about the use of their personal data is respected. The privacy notice on the corporate website is inaccurate in regard to the DPO role, does not include all required details and has not been reviewed since July 2018. We also identified a number of paper forms that collect personal data and do not have a privacy notice or has one that does not meet GDPR standards.

There is a procedure for dealing with subject access requests and other information rights, which are managed by the Information Management team. All requests are logged and the authenticity of the requesting person is confirmed as part of the process. There are no significant risks in this area.

The Information Security Management Policy and Procedure is out-of-date and hence a risk that data breaches are not effectively managed or reported. Specifically, that significant breaches may not be reported to the Information Commissioner's Office within 72hrs as required by UK GDPR.

Data Protection Impact Assessments (DPIA's) are performed to help identify and minimise the data protection risks of a project. There is a comprehensive template available to support these reviews but the process for carrying them out is not documented and hence roles, responsibilities and sign-off requirements are unclear. Our review of the process for completing the DPIA's identified issues around the recording of DPO comments.

There were 12 management actions agreed in the 2018/19 audit of GDPR, 11 of which have been closed by management on the basis of being implemented. The one outstanding action relates to having a documented retention policy as reported above. Of the 11 closed actions, we have identified two that have not been fully implemented, which relate to a review of 'consent' and the completeness of Information Asset Registers. These have been raised again in this report.