APPENDIX 1

Report	Summary of key findings and recommendations	Recommendations			Status
		H	M	L	
Subject: Information Governance Category: Assurance – Cyclical Date issued: 26 May 2023 Draft 16 August 2023 Final Level of Assurance: Satisfactory (Henderson Loggie LLP completed report equivalent to Midlothian Council Audit Substantial)	The EU General Data Protection Regulation (GDPR), which came into force on 25 May 2018 and was enshrined in law as part of the Data Protection Act 2018 (DPA 2018), included an expanded definition of what personal data was, a greater number of specific responsibilities, and implemented significant fines for non-compliance. The EU GDPR no longer applies in the UK after the end of the Brexit transition period on 31 December 2020. With effect from 1 January 2021, the DPPEC (Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit)) Regulations 2019 amended the EU GDPR to form a new, UK specific data protection regime that works in a UK context after Brexit to sit alongside the DPA 2018. This new regime is known as 'the UK GDPR'. Organisations are expected to control ever-increasing data volumes as developments in information technology allow data to be efficiently collected, stored and analysed. This elevates the risks within information management as the scope for mismanagement increases with the volume of data. Modern responses to information risk management include the incorporation of information governance. Good information governance practices take into account several considerations including: storage, communication & transference of information, compliance with laws, training and performance reporting. Storage, communication and transference of information should be supported by a reliable IT infrastructure with developed cybersecurity enhancements. Although ultimately solutions for information storage and communication is highly dependent on organisational needs, nonetheless whether cloud or physical servers are used these should be robust in order to avoid cybersecurity breaches. The storage of both carbon copy and electronic information requires retention schedules to be considered, often this in the form of a centralised list of data assets identifying how long the data asset is kept and when they are expected to be destroyed. Retention schedules are one of the requirements under UK GDPR as personal data is often contained within information held by the organisation. Under UK GDPR organisations are required to provide data subjects access to their personal data when a Subject Access Requests is made. This must be fulfilled	0	3	1	Management have accepted the factual accuracy of the report and its findings, and agreed to implement the recommendations.

Report	Summary of key findings and recommendations	Recommendations			Status
		H	M	L	
	within one calendar month of the request. Subject Access Requests (SARs) can be resource intensive where multiple SARs are received. The Council has established a robust data protection compliance framework, which includes a suite of policies, procedures, guidance, privacy notices, Information Asset Registers (IARs), data breach and Subject Access Request reporting and monitoring arrangements. A Data Protection Officer (DPO) is in place however the function is undertaken on an interim basis by the Information Compliance Officer who is a contractor with no access to contingency capability. The Henderson Loggie Internal Audit report provided Satisfactory assurance over the adequacy and effectiveness of controls and processes for information governance and the extent to which risks in this area are managed, specifically in the following areas: • Policy and procedures; • Roles and responsibilities; • Information requests; • Data processing; • Information communication; • Staff training; and • Management information and reporting. The Internal Audit report on Information Governance made the following recommendations: • A timetable should be developed to formal review and update of IARs, DPIAs and Privacy Notices within an achievable timescale. Suitably experienced senior staff within each service area should review the completeness and accuracy of information recorded in the IARs, DPIAs and Privacy Notices and update this information as required. This process should be completed annually and on completion each Executive Director should provide positive statement of assurance to the DPO. (Medium) • A review of the resources available for information governance should be completed in order to provide assurance of appropriate resource coverage in				

Report	Summary of key findings and recommendations	Recommendations			Status
		H	M	L	
	Data Protection and Records Management requirements across the Council. (Medium) • In line with the approach previously considered by the Council, the establishment of a network of data protection champions should be considered within each directorate to support the information management compliance within services. Specific areas of responsibility for data champions should include: ➢ Maintaining the accuracy of IARs; ➢ Assisting with DPIAs and Privacy Notices and ensuring that they remain current and up-to-date; ➢ Assisting in responding to SARs; ➢ Reviewing compliance with retention schedules; and ➢ Providing service specific data protection updates to their relevant teams. A programme of suitable training should be developed to support data champions to be effective in their roles (Medium) • An annual Data Protection Compliance report should be developed and formally reported to the CMT and Audit Committee. The report should include relevant data protection progress updates, as well as summarising key compliance metrics and trend analysis relating to data breaches, subject access requests and completion rates for staff training. (Low)				