Appendix One

Audits
Audit: Corporate Risk Register- General Data Protection Regulation (GDPR) 2022/2023 **Introduction:** The Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR) came into effect on 25 May 2018. The Council must comply with all relevant legislation and maintain good practices to protect the personal data held. A significant amount of work was undertaken prior to this date to ensure the Council was broadly compliant and this work is ongoing to maintain compliance. The Council has an approved Data Protection Policy that provides guidance to ensure that all personal data is lawfully processed by the Council and meets the seven key principles of the regulations. Non-compliance can result in potential fines form the Information Commissioner's Office (ICO) and compensation claims by an individual. As such, GDPR is included as a key risk on the council's corporate risk register.

Risk identified:	Level of Control:	Overall opinion:	Recommendations:
O1: Key controls stated in the corporate risk register in respect of GDPR planning are not in place and/ or working effectively	Substantial	Risks identified on the council's corporate risk register are regularly reviewed and commented upon by Corporate Management Team. In addition, the risk register is presented to and considered by the Audit and Governance Committee on a quarterly basis. General Data Protection Regulation is being managed as a key risk within the corporate risk register. Adequate mitigating controls have been identified to manage this risk and audit testing concluded the following in respect of their implementation: One of the mitigating controls of the Corporate Risk Register for GDPR is the regular review and update of the GDPR Action Plan, which is reviewed regularly by the Information Governance Board. **Corporate Risk Register** The terms of reference of the Audit and Governance Committee provide that Members gain assurance that key risks of the Council are being effectively managed. This is achieved through the risk management framework and associated Corporate Risk Register. The latest version was presented to the Committee on 23rd November 2022. The risk in respect of General Data Protection Regulation is identified in this document is recorded as follows: *'If the Council is not compliant with General Data Protection Requirements, then*	None required

there is a risk of financial penalties and adverse publicity'.

To mitigate this risk, controls are in place as shown below. Whilst it is not possible to completely reduce the likelihood of the risk crystalising, or the resulting impact, we can provide assurance that they are proportionate and are operating effectively.

Data Protection Policy

There is a Data Protection Policy, which is due to be updated and presented to the Audit and Governance Committee in March 2023.

Governance Structure

There is a strong governance structure, with key roles and responsibilities assigned and an Information Governance Board which meets regularly.

Breach Reporting Framework

A data breach reporting framework is in place that sets out the actions to be taken in respect of data breaches.

Staff Awareness Training

Staff have undertaken GDPR training and continue to particate in e-learning annually. Members were trained prior to the implementation of GDPR and will all be required to undertake e-learning after May 2023.

Regarding the GDPR risk management action points, appropriate and timely action has been taken as follows:

Rollout of e-learning module

An e-learning training package has been rolled out across the Council with all staff required to undertake this annually. Members are due to undertake e-learning in May 2023, after the local elections.

Implementation of Audit Recommendations

The follow up audit, undertaken in August 2021 confirmed that recommendations had been implemented and the risks identified mitigated.

Review of Data Protection Policy

The Data Protection Policy will be updated and presented to the Audit and Governance Committee in March 2023

	Reasonable	**GDPR Action Plan** The GDPR Action Plan is reviewed regularly by the Information Governance Board, to confirm that agreed actions remain appropriate, to identify new risks and to ensure that agreed timescales for completion are met. Our review of the Action Plan confirmed that several actions have been completed or are in progress. It was also found that some completion dates have been extended, for example: • Review of previous data audit - completion date was September 2022, now July 2023 – review in progress • Develop guidance of privacy impact assessments - completion date was July 2022, now October 2023 – review not started The plan is risk based to prioritise actions – the Council has a Single Point of Contact (SPoC) to deal with information governance. An update on the action plan and management of GDPR is presented annually to Audit and Governance Committee by the Council's Data Protection Officer.	

Recommendations Rating

Priority:		Definition:
1	**High**	A fundamental weakness in the system that puts the Authority at risk. This might include non-compliance with legislation or council policy,or may result in major risk of loss or damage to council assets, information or reputation. Requires action as a matter of urgency; to be addressed within a 3-6 month timeframe wherever possible or within an extended time frame as agreed with Internal Audit if the recommendation requires extensive resources or time.
2	**Medium**	Observations refer mainly to issues that have an important effect on the system of internal control but do not require immediate action. Legislation or policy are unlikely to be breached as a consequence of these issues, although could cause limited loss of assets, information or adverse publicity or embarrassment. Internal audit suggest improvement to system design to minimise risk and/or improve efficiency of service. To be resolved within a 6-9 month timescale.
3	**Low**	Observations refer to issues that would if corrected, improve internal control in general and ensure good practice, but are not vital to the overall system of internal control. A desirable improvement to the system, to be introduced within a 9-12 month period.

Level of control

Level of control:	Definition:	Guidance:
Substantial	Substantial assurance- A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.	No audit recommendations or no more than 3 low priority (3) recommendations.
Reasonable	Reasonable assurance- There is generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.	No more than 2 medium priority (2) recommendations, possibly with some low (3) recommendations.
Limited	Limited assurance- Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.	Between 1 and 3 high priority (1) and possibly several other priority recommendations OR 3 or more medium (2) recommendations.
No Assurance	No Assurance- Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.	4 or more Priority 1s OR 6 or more medium priority (2) recommendations.