Appendix 3

Internal Audit Report

Subject:	**Data Protection**
Date of Issue:	**28th May 2024**
Assurance Level Provided:	**Limited Assurance**

Report Distribution:	**Chief Executive** **Director of Corporate and Customer Services** **Director of Resources**

1.0 Introduction

1.1 In accordance with the 2023/24 Internal Audit Operational Plan a review of Data Protection arrangements has been undertaken.

2.0 Scope and Objectives

2.1 Due to the lack of progress made on implementing previously agreed audit recommendations and a number of areas identified for improvement as part of the independent review undertaken in March 2023 it was agreed with the Director of Corporate and Customer Services that no audit testing would be undertaken and that a report to document the current situation would be prepared. Areas reviewed as part of this audit included: -

- The implementation of previous audit recommendations
- Independent review of Data Protection Arrangements
- Management Response

3.0 Risks

3.1 The following risks to meeting the objectives have been considered.

- Noncompliance with Data Protection Act (DPA) 2018, General Data Protection Regulations (GDPR), Information Commissioner's Office (ICO) legislation
- Data asset mapping / Record of Processing Activities
- Data breaches leading to financial penalties
- Loss of data
- Lack of awareness by employees handling data

4.0 Conclusion

4.1 The conclusion of the audit was that the reliability of the internal controls relating to the above areas was assessed as **Limited Assurance** (Certain important controls are either not in place or not operating effectively. There is a risk that the system may not achieve its objectives. Some key risks were not well managed). For a full list of Assurance definitions linked to risk see Appendix 1.

4.2 The reason for this assurance level is primarily: -

- Data Protection continuing to be an area of risk documented on the annual governance statement,
- Five out of the eleven recommendations made during the previous audit review (2020) remain only partially implemented or outstanding,

- The external review in March 2023 identified 67 areas of non-compliance against the ICO Accountability Tracker.

5.0 Previous audit recommendations

5.1 During the previous data protection audit completed in September 2022 eleven recommendations were made. The implementation of these recommendations is as follows: -

Summary of recommendations	
Completed	6
In progress	3
Outstanding	2

Recommendation		Management Response – Sept 2020	Position as at March 2024
1	To ensure the Data Protection Policy is easily accessible to employees a dedicated Information Governance section should be established on the SIDD intranet site and this policy be included ***(Priority: Low)***	New policy approved but needs to be updated for accessibility before can be posted on website and SIDD. New section for Data Protection will be created on SIDD when new SIDD is ready.	Completed - Data Protection Policy (August 2022) is available on SIDD.
2	Contracts of employment and job descriptions should be updated to reflect the current Data Protection Act 2018, not Data Protection 1998 ***(Priority: Low)***	Human Resources Manager confirmed that all new contracts will include reference to the Data Protection Act 2018.	Completed - Contracts of employment refer to Data Protection Act 2018
3	Completion of the mandatory data protection training should be monitored to ensure that the training is completed by office-based employees. Training requirements for non-	LOLA training for office-based employees currently underway (deadline 30 Sept); completion being monitored by Information Governance Officer.	LOLA training for office based employees completed. Training has been completed in March 2024 for employees located at the ABC.

Recommendation		Management Response – Sept 2020	Position as at March 2024
	office based employees should be developed along with a process for recording who has received training. Consideration be given to removing computer access to those employees that have not completed the training by the target date. ***(Priority: High)***	Dates set for member training (12 Oct & 5 Nov) Dates for training for non-office based staff to be agreed.	Dates have been set for training to be provided to the Clean and Green team. Confirmed as at 10/04/24 this has now been completed for all non-office based staff.
4	As recommended by the ICO redaction training for employees should be provided. ***(Priority: Medium)***	Information Governance Officer to undertake the training first then train others where required.	Redaction training has now been completed for key employees (28), mop-up sessions to be arranged to capture remaining few.
5	To ensure all the data processing functions within a new system are fully documented/captured and reviewed adequately the DPIA must be completed by the project/service manager. The IGO should only provide advice regarding compliance and not be actively involved in the completion of the DPIA ***(Priority: Medium)***	Information Governance Officer to develop processes and hold a workshop and explain roles.	DPIA processes have been developed and a library of guidance and forms have been produced to assist staff in completion. The documents require an overarching procedure to be formalised and made available to staff on SIDD.
6	Training should be provided to designated officers to raise awareness of the requirement to complete a DPIA and to ensure that that the	As above	Due to lack or resource in the Information Governance Team, no training has taken place, however guidance has been formulated.

Recommendation		Management Response – Sept 2020	Position as at March 2024
	process captures and addresses data protection and privacy implications ***(Priority: Medium)***		Training material has been collated and a policy is in draft. Captured who needs training. Policy to be presented to CLT and anticipated that training can be completed by June 2024 to SLT.
7	Paper and electronic forms used by the Council which include personal information should be reviewed as soon as practically possible and amended to include a simpler statement on how their personal data will be dealt with and where they can find further information. To comply with Article 13 of GDPR a full more in-depth statement should be written and made available to individuals at the time we obtain their data. ***(Priority: Medium)***	Major project that will require training & support from all departments. First step is to produce briefing paper for CLT.	Review of all forms still required. External review in March 2023 stated that there had been no assessment of service level privacy notices to ensure they were compliant with DPA 2018.
8	The current asset register should be reviewed and updated to ensure that all personal data collected and processed by the authority can be recorded and	If less than 250 employees, asset register only needs to include routine processing. Therefore, we need to establish which processing is routine.	Identified as part of external review that no policy exists for Asset Management and that Personal Data Asset Register was last reviewed in 2018. Asset registers require the input of Directors and

Recommendation		Management Response – Sept 2020	Position as at March 2024
	mapped ***(Priority: Medium)***	First step is to produce briefing paper for CLT re "living" register to be on X drive for managers to maintain.	Service Managers to identify systems being used, data being captured and basis for processing.
9	Information Asset Owners and all employees must be reminded of the need to destroy paper records and delete electronic files in accordance with the data retention policy ***(Priority: Low)***	Information Governance Officer to remind information asset owners	Email circulated October 2020 to all employees regarding the data retention policy requirements
10	In accordance with the Document Retention Policy and to ensure that it can be evidenced that records containing personal information have been destroyed the requirement to complete the disposal certificate must be brought to the attention of all employees ***(Priority: Medium)***	Information Governance Officer to remind information asset owners	Email circulated October 2020 to all employees regarding the data retention policy requirements
11	The Council should continue its efforts to work towards achieving the PCI-DSS standard ***(Priority: Low)***	On hold pending new telephony solution	The Council not currently compliant on any card payment system. Due to the complexity and number of card payment channels the Council use. The Digital Transformation Project Manager is requesting approval to procure an external qualified assessor to progress the work needed to gain compliance.

6.0 External Review

6.1 The Council's previous Information Governance Officer (IGO) left the employment of the Council in August 2021. The temporary IGO who had been employed to assist the outgoing IGO was made permanent on 6 December 2022. Additional resource is provided by the Business Support Unit to support the IGO.

6.2 Due to resource capacity the IGO has primarily been concentrating their time on the statutory requirements of the role to ensure compliance with Information Commissioners Officer (ICO) requirements. This includes data breaches, subject access requests, third party requests and individual rights requests all of which have statutory timescales for completion.

6.3 In March 2023 an external review of data protection arrangements in operation at the Council was undertaken by DataSafe Assist. The review determined the Council's compliance status against the Information Commissioners Office (ICO) Accountability Tracker.

6.4 The table below shows compliance against each theme: -

Theme	Total number of expectations	Fully meets	Partially meeting	Not meeting	Not applicable
Leadership and oversight	33	7	17	3	6
Policies and procedures	17	1	12	3	1
Training and awareness	21	6	11	4	0
Individuals' rights	42	20	22	0	0
Transparency	31	16	3	5	7
ROPA and lawful basis	33	7	6	11	9
Contract and data sharing	31	0	9	19*	3
Risks and DPIA's	29	2	25	2	0
Records management and security	63	42	8	13	0
Breach response and monitor	38	30	1	7	0

*14 of the 19 not meeting expectations was reported as no evidence was presented during the review to determine compliance.

6.5 A summary of 'not meeting' expectations which was prepared as part of the external review report can be found at appendix 3.

6.6 Discussions with the Information Governance Officer at the time of writing this report highlighted that work is still progressing to address the 'not meeting' expectations but little progress has been made due to lack or resource.

7.0 Management Response

7.1 A report was presented to Council on 28 September 2023 to discuss a series of issues relating to organisational resilience. A recommendation was made as part of that report to commission external support for the re-writing of polices and to deliver training. A budget of £10,000 was included as part of the recommendation and was approved by Members.

7.2 It was confirmed during this audit review that no external support was procured following the report to Council in September 2023 due to the preferred supplier not having capacity to undertake the work. However due to the passage of time it has now been confirmed that the external consultant who completed the review detailed in paragraph 6.3 of this report now has availability to work on a contracted part time basis (provisionally 2 days per week). It is envisaged that this additional support will focus on the implantation of the outstanding internal audit recommendations and the areas of non-compliance against the ICO Accountability Tracker. This temporary arrangement is anticipated to commence in June 2024. The cost of this service will be met from the remaining budget of the £10,000 approved by Council (circa £9,200).

7.3 The Director of Corporate and Customer Services has disclosed that a report is to be presented in the coming weeks to the Corporate Leadership Team to seek permission to add an additional post of Governance Manager to the establishment. The role will include responsibility for Data Protection and will increase resource within this area.

	Recommendation
R1	It is essential that the outstanding audit recommendations and ICO expectations highlighted as being not meet by the external review are implemented and addressed as a matter of urgency ***(Priority: High)***

Internal Audit Report – Implementation Schedule

Report Title:	Data Protection	**Report Date: 28th May 2024**
		Response Due By Date: 18th June 2024

	Findings and Risk identified	Recommendations	Priority (High, Medium, Low)	Agreed	To be Implemented By:		Comments
					Officer	Date	
R1	Findings Internal Audit recommendations remain outstanding and an external review has also identified that legislative requirements have not been met. Risk Sanctions from Information Commissioners Office and financial penalties	It is essential that the outstanding audit recommendations and ICO expectations highlighted as being not meet by the external review are implemented and addressed as a matter of urgency	**High**		HJM	October 2024	A programme of work has been scoped and is ready for delivery in the short term by an interim contractor. Proposals have been made to CLT in which to create a Governance Manager role to provide the requisite capacity and capability into the service for the long term.

Please tick the appropriate response (✓) and provide comments for all recommendations not agreed.

Director:	HJM	Date:	5 June 2024

Note: In respect of any High priority recommendations please forward evidence of their implementation to the Internal Audit team as soon as possible.

Appendix 1

Derbyshire Dales District Council

Assurance Level	Internal Audit Definition	Risk Register Link
Substantial Assurance	There is a sound system of controls in place, designed to achieve the system objectives. Controls are being consistently applied and risks well managed.	Rare impact
Reasonable Assurance	The majority of controls are in place and operating effectively, although some control improvements are required. The system should achieve its objectives. Risks are generally well managed.	Possible / Unlikely impact
Limited Assurance	Certain important controls are either not in place or not operating effectively. There is a risk that the system may not achieve its objectives. Some key risks were not well managed.	Major impact
Inadequate Assurance	There are fundamental control weaknesses, leaving the system/service open to material errors or abuse and exposes the Council to significant risk. There is little assurance of achieving the desired objectives.	Critical Impact

Appendix 2

Definitions of High Medium and Low Recommendations

Rating	Definition
High	**Critical / Major: -** • **Personal Safety – Death** • **Substantial Financial Loss – for legal obligation claim / fine / custodial sentence / business loss claim / fine** • **Personal privacy infringement – All / severe personal details compromised** • **Reputation – Officers / Members forced to resign, local or public interest/national press aware** • Severe service disruption or regular disruption affecting more than one or all services • The Majority or all of Council priorities would be delayed or not delivered • High risk of fraud being able to occur e.g., key internal controls are not operating or are missing • Direct link to a strategic risk occurring • A serious breach of legislation/ legal requirements leading to substantial financial penalties or reputational damage • Substantial loss or damage to Council assets/or information
Medium	**Moderate: -** • **Personal Safety – injury outpatients** • **Moderate Financial Loss - for legal obligations claim / fine / business loss claim / fine** • **Personal privacy infringement – isolated, personal detail compromised** • **Reputation – Subject to formal report to Council** • Regular disruption to the activities of one or more council service • A number of Council priorities would be delayed or not delivered • Moderate Risk of fraud being able to occur • Direct link to identified operational risks occurring • A serious breach of organisational policies and procedures • A breach of legislation / legal requirements • Loss or damage to Council assets, information • Previously agreed medium internal audit recommendations remain outstanding
Low	**Low: -** • **Minor injury not serious, minor first aid** • **Low Financial loss for legal obligations claim / fine / business loss claim / fine** • **Personal privacy infringement – embarrassment, none lasting effect** • **Reputation – Contained within section / department** • • Some temporary disruption of activities of one Council Service • Some loss of trust and confidence in the Council felt by a certain group or within a small geographical area • It may cost more or delay in delivery of one of the Council's priorities • Low Risk of fraud • No direct link to operational or strategic risks • A minor breach of Legislation / legal requirements • Low risk of loss or damage to Council assets
Advisory	**Not risk or control related** • May enhance the service • May achieve efficiencies • May lead to an improved outcome

Appendix 3

Summary of ‘not meet’ – Indicates that the legislative requirements have not been met.

1	DPO expert knowledge and comprehensive JD/PS based on Article 39
2	Complete DP/IG library of policy and procedures with roles and responsibilities clearly documented, regularly reviewed, in a standard format with version control.
3	Ownership of the DP/IG training programme, with regular content reviews including IAO training, process to incorporate staff feedback
4	Information Asset Management Programme exists in order to maintain Information Asset Register, Record of Processing Activities and Privacy notices.
5	Organisation wide consent process.
6	Central data sharing log and guidance advising staff to record sharing decisions
7	Central log of data processors and contracts incorporating DP/IG requirements
8	Specific DPIA and Information Risk training for all staff
9	Records Management expertise and practices
10	Data quality reviews
11	Business Continuity Plan – specific to business data
12	Internal Audit Programme for DP /IG
13	KPI’s related to training completion rates

Internal Audit Consortium – Customer Satisfaction Survey

To assist Internal Audit to continually improve its service please complete the following questionnaire and return it together with the Implementation Schedule to Jenny Williams – Head of the Internal Audit Consortium. Thank you.

Report Title: Data Protection	**Date: 28th May 2024**

Ratings:
5= Very Good, 4= Good, 3= Satisfactory, 2= Needs Improvement, 1= Unsatisfactory

Planning		**Rating**
1.	How well were the risks, scope and objectives discussed with you?	**5**
2.	Was the notification of the audit start date appropriate and adequate?	**5**

Conduct

3.	Was the conduct of the audit planned and undertaken in a way that caused you minimum disruption?	**5**
4.	Was the Auditor courteous and professional?	**5**
5.	Was the audit completed in a manner that showed a good knowledge of the area audited?	**5**
6.	Did you receive adequate feedback of the findings during the audit?	**5**

Report

7.	Was the report fair and accurate in its findings and the recommendations practical and realistic?	5
8.	Was the report clearly set out, presented and readily understood?	5
9.	Was the report sent to you promptly?	5

General

10.	What was your overall satisfaction with the audit service?	**5**

Additional Comments

A*S ever. A great service.*

Survey Completed By: HJM	**Date:**
	28/5/2024