REPORT TO: **TAYSIDE VALUATION JOINT BOARD – 21 NOVEMBER 2022**

REPORT ON: **INTERNAL AUDIT**

REPORT BY: **ASSESSOR**

REPORT NO: **TVJB 19-2022**

1 PURPOSE OF REPORT

1.1 To present to the Board the following Internal Audit Report which is attached as an appendix to this report:-

Internal Audit Report 2023/03 – Data Protection/Freedom of Information

2 RECOMMENDATIONS

2.1 The Joint Board is asked to note the contents of this Report and attached Audit Report.

3 FINANCIAL IMPLICATIONS

3.1 The cost of Internal Audit Services is provided for in the Assessor's Revenue Budget.

4 POLICY IMPLICATIONS

4.1 This report has been screened for any policy implications in respect of Sustainability, Strategic Environmental Assessment, Anti Poverty, Equality Impact Assessment and Risk Management. There are no major issues.

5 BACKGROUND

5.1 Henderson Loggie, Chartered Accountants, were appointed to provide an Internal Audit Service in respect of the financial years 1 April 2022 to 31 March 2025. Audit work has proceeded in accordance with the Audit Needs Assessment and Strategic Plan for the period 2022 to 2025 as approved by the Joint Board on 29 August 2022.

5.2 Internal Audit Report 2023/03 – Data Protection/Freedom of Information - is attached as Appendix 1 to this report. It has been prepared by Internal Audit following discussion with the Assessor. The overall conclusion of the report is that the level of assurance is good and that the system meets the control objectives. Two opportunities for improvement have been identified however, and the Assessor will now work to ensure these improvements are made.

6 CONSULTATIONS

6.1 The Clerk and Treasurer to the Joint Board have been consulted on this report.

7 BACKGROUND PAPERS

7.1 None.

ROY CHRISTIE
Assessor **November 2022**

APPENDIX

LEVEL OF ASSURANCE
Good

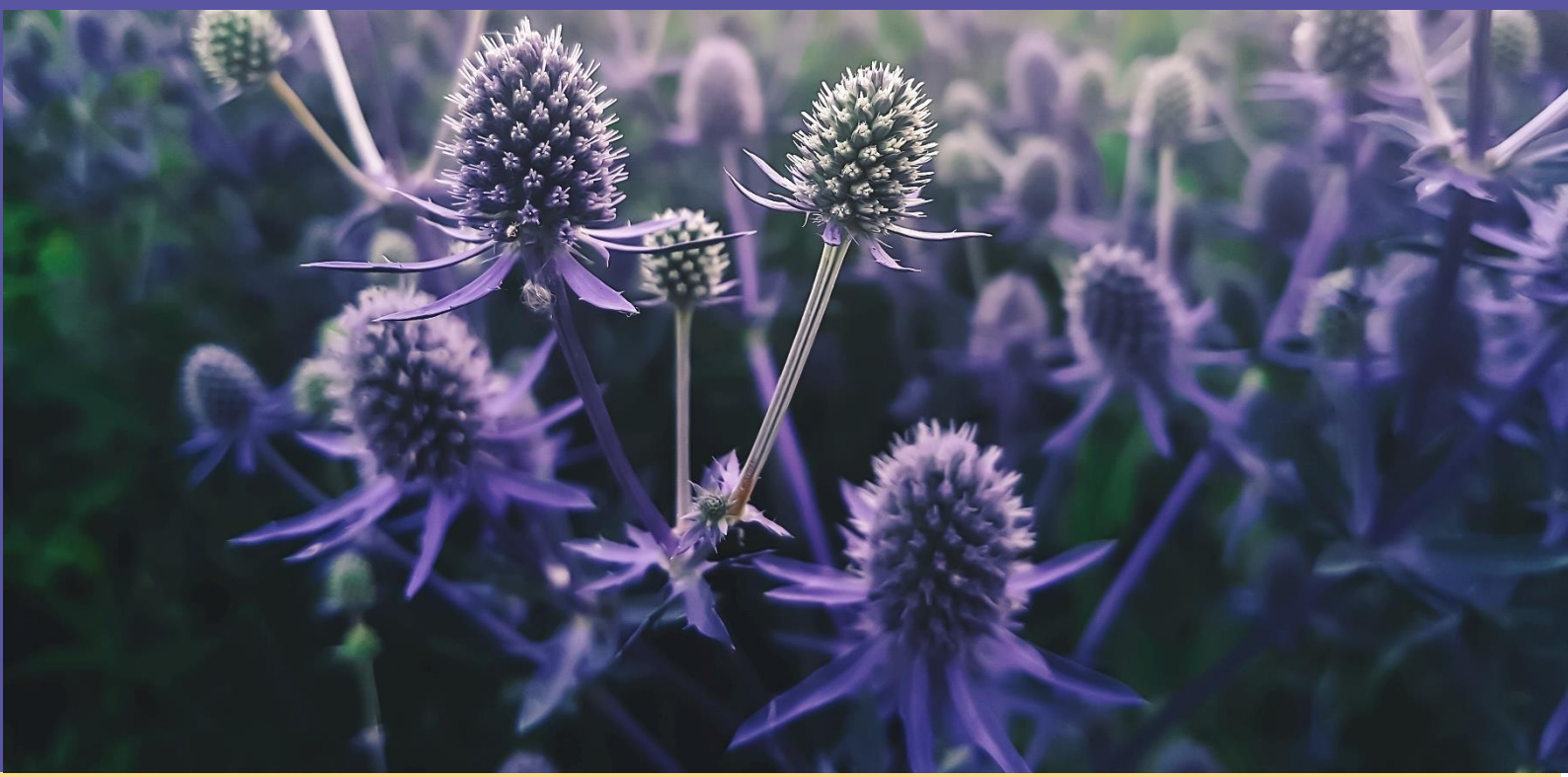
Tayside Valuation Joint Board

Data Protection / Freedom of Information

Internal Audit report No: 2023/03

Draft issued: 10 November 2022

Final issued: 10 November 2022



Henderson Loggie

		Page
Section 1	**Management Summary**	
	• **Overall Level of Assurance**	**1**
	• **Risk Assessment**	**1**
	• **Background**	**1**
	• **Scope, Objectives and Overall Findings**	**2**
	• **Audit Approach**	**2**
	• **Summary of Main Findings**	**2 - 3**
	• **Acknowledgements**	**3**
Section 2	**Main Findings**	**4 - 8**

Level of Assurance

In addition to the grading of individual recommendations in the action plan, audit findings are assessed and graded on an overall basis to denote the level of assurance that can be taken from the report. Risk and materiality levels are considered in the assessment and grading process as well as the general quality of the procedures in place.

Gradings are defined as follows:

Good	System meets control objectives.
Satisfactory	System meets control objectives with some weaknesses present.
Requires improvement	System has weaknesses that could prevent it achieving control objectives.
Unacceptable	System cannot meet control objectives.

Action Grades

Priority 1	Issue subjecting the organisation to material risk, and which requires to be brought to the attention of the Joint Board.
Priority 2	Issue subjecting the organisation to significant risk, and which should be addressed by the Assessor.
Priority 3	Matters subjecting the organisation to minor risk or which, if addressed, will enhance efficiency and effectiveness.

Management Summary

Overall Level of Assurance

Good	System meets control objectives.

Risk Assessment

This review focused on the controls in place to mitigate the following risks on the Tayside Valuation Joint Board ('the Board') Strategic Risk Register:

- 5.1 – Legislative changes affecting: General Data Protection Legislation (GDPR) (risk rating: low)

Background

As part of the Internal Audit programme at the Board for 2022/23, we carried out a review of the data protection and freedom of information processes in place. Our Audit Needs Assessment identified this as an area where risk can arise and where Internal Audit can assist in providing assurances to the Joint Board and Assessor that the related control environment is operating effectively, ensuring risk is maintained at an acceptable level.

The Data Protection Act 2018 (DPA) sets out the framework for data protection law in the UK. It updated and replaced the Data Protection Act 1998 and came into effect on 25 May 2018. It was amended on 1 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU. It sits alongside and supplements the UK GDPR.

The UK GDPR includes an expanded definition of what personal data is; includes a greater number of specific responsibilities; and has implemented significant fines for non-compliance. One of the key aspects of the updated legislative duties is the accountability principle, in that an organisation must show how it complies with the data protection principles, with a focus on comprehensive but proportionate (risk-based) governance measures that should minimise the risk of breaches and uphold the protection of personal data.

The Freedom of Information (Scotland) Act 2002 (FoI(S)A) came into effect on 1 January 2005, entitling individuals to see information held by public authorities as defined by the Scottish Information Commissioner. This includes information recorded on paper, computer files (including e-mails), video and microfiche. Under the FoI(S)A, all Scottish public authorities have a statutory obligation to respond to FoI requests within 20 working days; however, authorities have the right to withhold information if it falls under one of the exemptions listed in the FoI(S)A. Where information is withheld, the reasons for non-disclosure must be notified to the individual making the request.

Under the FoI(S)A the Board is required to have its own Publication Scheme, which is accessible on the Board's website, as a guide to the information available; where it can be found; and whether or not it is available free of charge.

Scope, Objectives and Overall Findings

The audit focused on the arrangements in place within the Board to ensure compliance with key requirements of the Data Protection Act 2018, the UK General Data Protection Regulation (GDPR) and the Freedom of Information (Scotland) Act 2002.

The table below notes each separate objective for this review and records the results:

Objective	Findings			
The specific objectives of the review were to ensure that:		**1**	**2**	**3**
		No. of Agreed Actions		
1. Appropriate action has been taken by the Board to comply with the Data Protection Act 2018, including the UK GDPR, and Freedom of Information (Scotland) Act 2002; and	**Good**	0	0	1
2. Adequate procedures are in place for the ongoing monitoring of compliance with data protection and freedom of information legislation.	**Satisfactory**	0	0	1
Overall Level of Assurance	**Good**	**0**	**0**	**2**
		System meets control objectives		

Audit Approach

Through discussion with the Assessor and the Data Protection Officer (DPO), and review of policies and procedures, we established the action taken to date by the Board, and any further action planned, to implement the applicable requirements of data protection and freedom of information legislation. The Information Commissioner's Office guidance was used as the basis for this discussion, and any additional action required will be highlighted.

Summary of Main Findings

Strengths

- A data protection compliance framework has been established which includes a suite of policies, procedures, guidance, privacy notices, information registers, data breach and Subject Access Request reporting and monitoring arrangements; and
- Independent advice and guidance on data protection legislation, and the Board's data protection arrangements, is provided by Dundee City Council's Information Governance Manager, who acts as the Board's appointed DPO.

Opportunities for improvement

- A number of data protection and FoI policies and procedures refer to the previous Assessor and Assistant Assessor and therefore now require to be updated. The Data Protection Policy also refers to the EU GDPR which, following the UK's departure from the EU, has now been brought into UK law and is commonly referred to the 'UK GDPR'; and
- The form, frequency and method of ongoing compliance monitoring has still to be formalised which reflects existing practices, including: periodic gap analysis and treatment plan exercises; the interaction between the DPO and the senior management team; monitoring of completion of the online data protection training module; data protection briefings and guidance provided by the DPO; annual internal data protection compliance audits; and annual report on data protection matters to the Joint Board by the DPO.

Acknowledgment

We would like to thank Board staff for the co-operation and assistance we received during our review.

Main Findings

Objective 1: Appropriate action has been taken by the Board to comply with the Data Protection Act 2018, including the UK GDPR, and Freedom of Information (Scotland) Act 2002.

Data Protection
As noted on the Board's entry on the Information Commissioners' Office Data Protection Register, the Assessor, as Data Controller, is responsible for the implementation of the Data Protection Act 1998.

Our audit included a review of the specific data protection arrangements in place within the Board, in order to obtain reasonable assurance that robust procedures have been established, and are operating, to ensure ongoing compliance with data protection legislation. We reviewed the Board's key policies and procedures to obtain an understanding of the Board's compliance environment.

Dundee City Council's (DCC) Information Governance Manager has been appointed as the DPO for the Board. The DPO carried out a review of the Board's data protection compliance arrangements as part of the preparations for the implementation of the GDPR in 2018. The review also included the provision of guidance and awareness training to the Board's management team. Following the review, the Board was provided with an action plan to address any compliance gaps. The Board has continued to receive advice and guidance from the DPO as part of the Board's ongoing compliance with data protection legislation, although we did note that advice is sought in response to specific compliance issues which cannot be resolved by the management team, or through other channels such as the Scottish Assessors Association which provides advice on governance matters to all Assessors. We noted that the Board has developed appropriate and proportionate data protection procedures to ensure ongoing compliance with the legislation, including a records management plan.

The Board's data processing activities, data sources and categories of personal data, the lawful basis for processing each type of activity and data retention periods are largely governed by the Board's statutory functions and so the lawful basis for data processing is defined under various pieces of legislation and statutory instruments.

Online e-learning data protection and information security training modules are available to all staff which form part of the suite of mandatory induction training for all new staff. Staff are required to complete the package of induction training within three months of their employment start date.

Documented procedures to handling of subject access requests, data breaches and data protection impact assessments (DPIAs).

DPIAs have been undertaken as part of the implementation of new systems and technology to ensure that data protection risks are identified and mitigated.

There is regular reporting of data protection issues to the senior management team, and to the Board as they arise.

Objective 1: Appropriate action has been taken by the Board to comply with the Data Protection Act 2018, including the UK GDPR, and Freedom of Information (Scotland) Act 2002 (continued).

Freedom of Information
The Freedom of Information (Scotland) Act 2002 gives a general right of access to recorded information held by Public Authorities, sets out exemptions from that general right and places a number of related obligations on Public Authorities including the requirement to create and maintain a Publication Scheme and a Records Management Plan.

The Act applies to any records held by the authority no matter when they were created.Schedule 1 (Part 3) of the Freedom of Information (Scotland) Act 2002, lists those bodies and office holders which are, for the purposes of the Act, regarded as Scottish Public Authorities. The Assessor is appointed under Section 27(2) of the Local Government Etc. (Scotland) Act 1994 and is listed in Schedule 1 (Part 3) of the Freedom of Information Scotland Act, 2002. The Assessor is therefore a separate and distinct Scottish Public Authority. The Assistant Assessor has been appointed by the Assessor as the officer responsible for the Board's Freedom of Information administration.

We noted that publication schemes are in place for both the Board and the Assessor, as a well as a Records Management Plan.

We confirmed with the Assessor, who is assisted by the Assistant Assessor, that they had sufficient time available to meet their responsibilities and this was supported by the very low number of Freedom of Information requests which are received.

We reviewed the Board's Freedom of Information procedures, which set out what action should be taken in the event of receiving an information request and we confirmed that these procedures demonstrated a robust process.

The Board's Freedom of Information Guide to Staff and procedures for handling requests were compared against the Freedom of Information legislation and guidance from the Scottish Information Commissioner and the ICO to determine whether they adequately set out all requirements. From our review we concluded that the applicable requirements were covered.

Information on Freedom of Information forms part of the mandatory induction process for new staff.

Objective 1: Appropriate action has been taken by the Board to comply with the Data Protection Act 2018, including the UK GDPR, and Freedom of Information (Scotland) Act 2002 (continued). (Continued)

Observation	Risk	Recommendation	Management Response	
We noted that a number of data protection and FoI policies and procedures refer to the previous Assessor and Assistant Assessors. The Data Protection Policy also refers to the EU GDPR which, following the UK's departure from the EU, has now been brought into UK law and is commonly referred to the UK GDPR. The new Assessor recently came in to post and has, following a review, identified that policies and procedures require to be updated and refreshed.	Policies and procedures are not up to date and do not reflect current legislation, roles and responsibilities resulting in non-compliance or gaps in accountability.	**R1** When the opportunity allows, policies and procedures relating to data protection and freedom of information should be updated to reflect roles and responsibilities within the current structure, and to reflect current legislation and operational practices.	Management will review and update policies and procedures. **To be actioned by:** Assessor **No later than:** 30 June 2023	
			Grade	**3**

Objective 2: Adequate procedures are in place for the ongoing monitoring of compliance with data protection and freedom of information legislation.

An annual report on Freedom of Information and Environmental Information is reported to the Joint Board annually summarising the key controls and activities in the year.

The Assistant Assessor for East Division has been appointed by the Assessor as the officer responsible for the Board's Freedom of Information and Environmental Information. In addition, the Assessor is represented on the Scottish Assessors' Association Governance Committee which considers Freedom of Information and Environmental Information matters as they affect Assessors on a Scotland wide basis. The Assistant Assessor monitors Freedom of Information and Environmental issues on a national basis to ensure that the Board's requirements in relation to these matters are properly represented.

The Board has a Governance Group which is responsible for dealing with routine Freedom of Information and Environmental Information issues on behalf of the Assessor. The Group meets regularly, and its proceedings are formally minuted, with findings discussed at senior management team meetings as appropriate.

Objective 2: Adequate procedures are in place for the ongoing monitoring of compliance with data protection and freedom of information legislation. (Continued)

The Board maintain records of all data protection subject access requests and freedom of information (FoI) requests, and these are monitored to ensure that requests are actioned within the statutory timescales for providing responses. From a review of records and discussion with the Assessor, we noted that the Board receives very few of these types of requests. In 2022, the Board received no SARs and one FoI request.

Observation	Risk	Recommendation	Management Response	
Overall, the Board continues to implement the requirements of the data protection legislation, and data protection is a standing agenda item at senior management team meetings. One aspect of the DPO's role is to ensure that systems are in place for ongoing monitoring of data protection compliance. However, at the time of our review the form, frequency and method of compliance monitoring had still to be formalised which reflects existing practices, including: • regular gap analysis and treatment plan exercises; • the interaction between the DPO and the senior management team; • monitoring of completion of the online data protection training module; • data protection briefings and guidance provided by the DPO; • annual internal data protection compliance audits; and • annual report on data protection matters to the Joint Board by the DPO.	Without robust and effective procedures for monitoring and testing compliance with the Board's data protection policies, there is an increased risk of insecure data handling practices and potential data breaches not being detected in a timely manner. Fines may be imposed by the Information Commissioner's Office if it is found that data breaches could have been prevented if adequate monitoring procedures had been in place.	**R2** A data protection compliance monitoring procedure, and associated audit plan, should be formalised, which reflects and builds upon existing practices, and which identifies the form, frequency and method of compliance monitoring and describes how results should be reported. The DPO should be consulted when developing these procedures to ensure that they are both robust and proportionate for the Board.	Management will consult with DPO to develop and formalise a data protection compliance monitoring procedure and associated audit plan. **To be actioned by:** Assessor **No later than:** 31 August 2023	
			Grade	**3**

Henderson Loggie

Aberdeen 45 Queen's Road AB15 4ZN
Dundee The Vision Building, 20 Greenmarket DD1 4QB
Edinburgh Ground Floor, 11-15 Thistle Street EH2 1DF
Glasgow 100 West George Street, G2 1PP

T: 01224 322 100
T: 01382 200 055
T: 0131 226 0200
T: 0141 471 9870

F: 01224 327 911
F: 01382 221 240
F: 0131 220 3269

Henderson Loggie LLP is a limited liability partnership registered in Scotland with registered number SO301630 and is a member of PrimeGlobal, a global association of independent accounting firms, the members of which are separate and independent legal entities. Registered office is: The Vision Building, 20 Greenmarket, Dundee, DD1 4QB. All correspondence signed by an individual is signed for and on behalf of Henderson Loggie LLP. Reference to a 'partner' is to a member of Henderson Loggie LLP. A list of members' names is available for inspection at each of these addresses.