Board of Management

Audit & Assurance Committee

Date of Meeting	**3 March 2026**
Paper No.	**AAC3-G**
Agenda Item	**5.2.4**
Subject of Paper	**Internal Audit Report: Data Protection**
FOISA Status	**Disclosable**
Primary Contact	**David Archibald, Henderson Loggie**
Date of production	**19 February 2025**
Action	**For Discussion**

1. Recommendations

1.1. The Committee is asked to consider and discuss the report and the management responses to the Internal Audit Recommendations.

2. Consultation

2.1. The Lead Auditor has consulted with the Executive Owner, the College Lead, and the Compliance Auditor.

3. Key Insights

3.1. The Internal Audit for Data Protection has identified one Priority 3 recommendation from the fieldwork, which has a management response.

4. Impact and Implications

4.1. Internal Audit provides an objective insight into the efficiency of operations, evaluation of risks, and organisational controls.

Appendix 1: Internal Audit Report – Data Protection

LEVEL OF ASSURANCE
Good

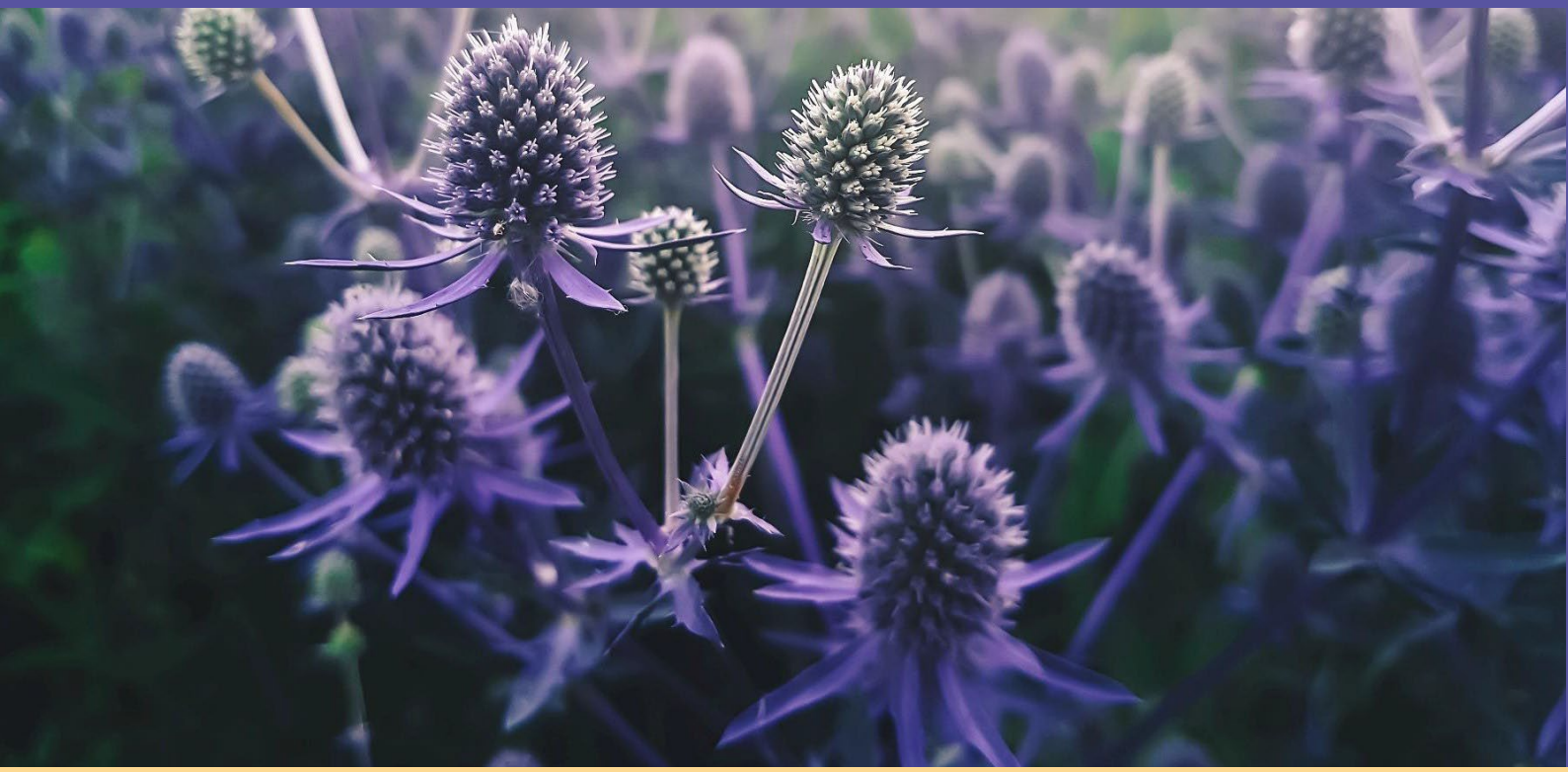
City of Glasgow College

Data Protection

Internal Audit report No: 2026/05

Draft issued: 09 February 2026

Final issued: 19 February 2026



Henderson Loggie

Contents

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 management and the Audit & Assurance Committee.
Priority 2	Issue subjecting the organisation to significant risk, and which should be addressed by management.
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 risk on the City of Glasgow College ('the College') Strategic Risk Register:

- SR12 – Negative impact of statutory compliance failure (risk rating: moderate); and
- SR14 – Failure of compliance with the General Data Protection Regulations (GDPR) (risk rating: moderate).

Background

As part of the Internal Audit programme at the College for 2025/26, we carried out a review of the systems in place in relation to Data Protection. The Audit Needs Assessment (ANA) identified this as an area where risk can arise and where Internal Audit can assist in providing assurances that the related control environment is operating effectively, ensuring risk is maintained at an acceptable level.

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.'

On 19 June 2025, the Data Use and Access Act 2025 ('DUAA') became law in the UK. This law sits alongside the UK GDPR and DPA 2018, and introduces some changes to data protection law in the UK. The College is assessing the impact of the DUAA on its processing activities and will implement necessary changes to ensure compliance.

Scope, Objectives and Overall Findings

We carried out a review of the College's implementation of the Data Protection Act 2018, including relevant aspects of the UK GDPR and DUAA, to ensure that processes and procedures are in place to allow compliance with these.

The table below notes the objectives for this review and records the results:

Objective		Findings		
		1	2	3
The objective of our audit was to obtain reasonable assurance that:		**No. of Agreed Actions**		
1. Appropriate action has been taken by the College to comply with the Data Protection Act 2018, including the UK GDPR and DUAA.	**Good**	-	-	1
2. Adequate procedures are in place for the ongoing monitoring of compliance with data protection legislation.	**Good**	-	-	-
		-	**-**	**1**
Overall Level of Assurance	**Good**	System meets control objectives.		

Audit Approach

Through discussion with the Depute Principal and Chief Operating Officer and the College's Data Protection Officer (DPO) we established the action taken to date by the College, and any further action planned, to implement the Data Protection Act 2018, including the requirements of the UK GDPR and DUAA. The Information Commissioner's Office guidance was used as the basis for this discussion.

Summary of Main Findings

Strengths

- The College has established a robust data protection compliance framework, which includes a mandatory programme of training for all staff supported by a suite of policies, procedures, guidance, privacy notices, Record of Processing Activities (RoPA) for each department, data breach and Subject Access Request reporting and monitoring arrangements; and mechanisms for identifying and assessing data protection risks.
- Senior College staff are responsible for all operational aspects of data protection who are supported by an external DPO.
- Monitoring processes are in place to maintain oversight of data protection compliance across the College, including regular data protection gap analysis performed by the DPO with results reported to the Executive Team and Audit & Assurance Committee.

Actions Already in Progress

- Through the regular data protection compliance gap analysis, and the review performed as part of this audit, some minor gaps in the information recorded in departmental RoPAs have been identified. However, data protection health check questionnaires will be issued to the relevant department leads in February 2026, with RoPAs then updated to ensure gaps have been addressed and submitted to the DPO for review by April 2026.
- The College does not currently have a relevant oversight group responsible for data protection compliance, however the College plans to establish an Information Governance Group by the end of the 2025/26 academic year, which will comprise staff from curriculum and support teams.

Opportunities for Enhancement

- No significant weaknesses were identified during our review.
- However, we noted that there is no central log of all Data Protection Impact Assessments (DPIA) that have been completed. Completion of a DPIA log would allow clearer visibility of DPIA ownership, and for any assessments that are related to recurring activities but are time limited, the DPIA log would capture details of the scheduled review dates.

Acknowledgments

We would like to take this opportunity to thank the staff at the College who helped us during our review.

Main Findings and Action Plan

Objective 1: Appropriate action has been taken by the College to comply with the Data Protection Act 2018, including the UK GDPR and DUAA.

Our audit included a review of the specific arrangements in place within the College to obtain reasonable assurance that robust procedures have been established, and are operating, to ensure compliance with extant data protection legislation. We reviewed key policies and procedures, and we also met with the Deputy Principal and Chief Operating Officer and the DPO to obtain an understanding of the College's compliance environment. We then reviewed the processes and controls established for identifying, processing, and securing personal data.

The College has developed a data protection framework, which incorporates data protection and information security training; records management, including access and retention; ICT security; risk identification and assessment; data sharing; governance; and compliance monitoring. The College's approach has been externally reviewed by the independent DPO, who continues to advise on ongoing compliance. The DPO has formed the view that the College is able to demonstrate a good level of data protection compliance.

Based on our review we are, overall, satisfied that the College has good data protection policies and procedures in place and several areas of good practice were identified, including:

- The College has developed a baseline record of its processing activities (RoPA) for each department which covers the key requirements of the GDPR / DPA, such as identifying where personal data has been collected from; the points within the organisation where personal data resides; data retention; data security classification; and data transfers with third parties. The findings documented on the RoPA have informed the development of the College's data protection related policies, procedures, privacy notices and data protection training and also the guidance made available to staff. Some minor gaps in the information recorded in departmental RoPAs exist. However, data protection health check questionnaires will be issued by the DPO to the relevant department leads in February 2026, with RoPAs then updated to ensure that identified gaps have been addressed.
- e-learning training modules, covering data protection and information security, 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. Review of compliance statistics noted a high level of staff (80%) had completed the mandatory training for the last full cycle of training completed in 2025. This figure is impacted by new staff members who have not yet completed their induction training and also by staff absences. The College demonstrated commitment to improving the compliance rate.
- Documented procedures for handling subject access requests, data breaches and data protection impact assessments.
- Guidance has been produced for staff, which includes the College's policies and procedures around the use, management, security, confidentiality and disclosure of information.

Objective 1: Appropriate action has been taken by the College to comply with the Data Protection Act 2018, including the UK GDPR and DUAA (continued).

Areas of good practice (continued):

- The DPO provides advice on the development of data protection related policies and procedures, data sharing agreements, reviews evidence of compliance and participates in the College's internal compliance checks. The DPO is further supported by departmental leads who liaise with the DPO on data protection matters and are responsible for completing the annual data protection health check questionnaires issued by the DPO.
- Data Protection Impact Assessments (DPIAs) have been undertaken as part of the implementation of new processes, systems and technology to ensure that data protection risks are identified and mitigated.
- All subject access requests (SARs) are made through a dedicated mailbox which the DPO has access to. We noted that SARs are managed directly by the DPO, including data gathering, reviewing, and redacting the data and responding to the data subject.
- A Data Protection Policy which reflects Information Commissioner's Office (ICO) guidance.
- Separate privacy notices are in place which reflects the range of data protection engagements with staff, students and stakeholders and reflects ICO guidance.
- Regular reporting of data protection issues as they arise to the Deputy Principal and Chief Operating Officer, Executive Team, and the Audit & Assurance Committee.

In November 2025, the DPO quarterly report to the Audit & Assurance Committee included the results of the College's data protection compliance gap analysis. This analysis is effectively a self-evaluation exercise against the ICO's Accountability Framework. The gap analysis summarised the College's compliance with the core aspects of the framework. The results showed that the College was fully meeting the ICO's expectations for data protection compliance in the majority of areas, and partially meeting expectations in the few remaining areas, including further development of governance structures, updating of RoPAs and retention of data. We noted that improvement actions have been agreed by the College to address these areas. Some minor gaps in the information recorded in departmental RoPAs exist. However, we were advised that data protection health check questionnaires will be issued by the DPO to the relevant department leads in February 2026, with RoPAs subsequently updated to ensure that any gaps identified have been addressed. The College does not currently have a relevant oversight group responsible for data protection compliance. However, we were advised that the College plans to establish an Information Governance Group by the end of the 2025/26 academic year, which will comprise staff from curriculum and support teams.

As part of our audit fieldwork, we separately completed the ICO's Accountability Framework based on our review of the College's data protection arrangements, including a review of evidence noted in this report. Our assessment confirmed that the College is meeting the ICO's expectations in almost all areas, again noting that there are opportunities for further improvements to be made in a small number of areas as noted in the College's most recent gap analysis reported in November 2025.

Based on our review we are, overall, satisfied that the College has established a robust data protection compliance framework.

Objective 1: Appropriate action has been taken by the College to comply with the Data Protection Act 2018, including the UK GDPR and DUAA (continued).

Observation	Risk	Recommendation	Management Response	
The College has put in place a structured assessment process for undertaking a Data Protection Impact Assessment (DPIA) to identify, evaluate, and mitigate privacy risks when the College plans to process personal data in ways that could pose a high risk to individuals' rights and freedoms. For all new significant projects involving the processing of personal data, an initial assessment is performed to determine risk levels and the need for a full DPIA. Where the level of risk is deemed to be high, a full DPIA is undertaken to fully record the processing activities and fully assess the protections and mitigations in place. Completion of DPIAs is performed by the DPO in conjunction with College staff responsible for the personal data processing activity. We noted from a review of the information captured in the RoPAs that links to DPIAs are provided. The results of DPIAs are held by the DPO but there is no central log of all DPIAs that have been completed. Completion of a DPIA log would allow clearer visibility of DPIA ownership, and for any that are related to recurring activities but are time limited, details of the scheduled review dates.	Without a central DPIA log, senior management or the DPO cannot track whether actions and mitigations have been completed, or ensure DPIAs are reviewed periodically.	**R1** Steps should be taken to implement a centralised Data Protection Impact Assessment (DPIA) log to record all DPIAs, including their status, outcomes, approvals, and associated mitigation actions. The log should be maintained by the Data Protection Officer and integrated into existing governance processes.	Management thanks the internal auditors for its comments and recommendation. Management agrees with the auditor's recommendation to implement a DPIA log to ensure the College can effectively demonstrate its compliance with Article 35 of UK GDPR. The log will be added to a dedicated Microsoft Teams site where it will be maintained by the Data Protection Officer, together with copies of DPIAs in progress and DPIA's completed to improve visibility. Reporting on the status DPIAs shall be periodic via the AAC. **To be actioned by:** Data Protection Officer **No later than:** 31 March 2026	
			Grade	**3**

Objective 2: Adequate procedures are in place for the ongoing monitoring of compliance with data protection legislation across the organisation which are sufficiently well developed to inform reporting to senior management and to the Audit and Risk Committee going forward.

The DPO plays a key role in the oversight and application of the College's data protection procedures, meeting regularly with the Deputy Principal and Chief Operating Officer to discuss relevant issues and challenges. One key aspect of the DPO's role is to ensure that the College has systems and procedures in place for ongoing application and monitoring of data protection compliance, although the DPO is not personally responsible for ensuring that those systems are being followed in practice. Whilst the DPO is actively involved in the College's compliance arrangements, the Deputy Principal and Chief Operating Officer maintains operational and day-to-day responsibility for monitoring implementation of the College's procedures and therefore maintains oversight of ongoing compliance with legislation. If required, data protection issues, including any significant instances of non-compliance with procedures or legislation, would be reported to the Executive Team and the Board via the Audit & Assurance Committee, with any improvement actions also communicated to staff as required. This includes quarterly reporting of the data protection compliance gap analysis results which highlight improvement actions.

As noted above under objective 1, the College does not currently have a relevant oversight group responsible for data protection compliance. However, the College plans to establish an Information Governance Group by the end of the 2025/26 academic year, which will enhance the College's compliance monitoring arrangements.

High level data protection metrics, (e.g. data breaches), are reported to the Board during the year. This provides an update on the College's performance in complying with its obligations under the data protection legislation.

Subject Access Requests (SARs) are recorded and monitored by the DPO. Metrics in relation to completing SARs within the one-month statutory timescales were provided for audit and we confirmed that all SARs received in 2025 discharged within one month, or by the agreed extended deadline.

Based on our review we are, overall, satisfied that the College has adequate arrangements in place for monitoring compliance with data protection legislation across the organisation.

Henderson Loggie

Aberdeen: 1 Marischal Square, Broad Street, AB10 1BL **T:** 01224 322 100
Dundee: The Vision Building, 20 Greenmarket, DD1 4QB **T:** 01382 200 055
Edinburgh: Level 5, Stamp Office, 10-14 Waterloo Place, EH1 3EG **T:** 0131 226 0200
Glasgow: Suite 5.3, Kirkstane House, 139 St Vincent Street, G2 5JF **T:** 0141 471 9870