Board of Management
Audit & Assurance Committee

Date of Meeting	**Tuesday 29 November 2022**
Paper No.	**AAC2-H**
Agenda Item	**5.6.3**
Subject of Paper	**Internal Audit Report – Data Protection**
FOISA Status	**Disclosable**
Primary Contact	**Henderson Loggie**
Date of production	**22 November 2022**
Action	**For Discussion and Decision**

1. Recommendations

The Committee is asked to consider and discuss the report and the management responses to the internal audit recommendations.

2. Purpose of report

The purpose of this review is to provide management and the Audit and Assurance Committee with assurance on key controls relating to the curriculum and financial plans in place for City of Glasgow College and their alignment with the regional plan for Glasgow and the college student number targets.

3. Key Insights

This internal audit of Data Protection provides an outline of the objectives, scope, findings and graded recommendations as appropriate, together with management responses. This constitutes an action plan for improvement.

The Report includes a number of audit findings which are assessed and graded to denote the overall level of assurance that can be taken from the Report. The 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.

4. Impact and implications

Refer to internal audit report.

Appendix – Internal Audit Report – Data Protection

LEVEL OF ASSURANCE
Satisfactory

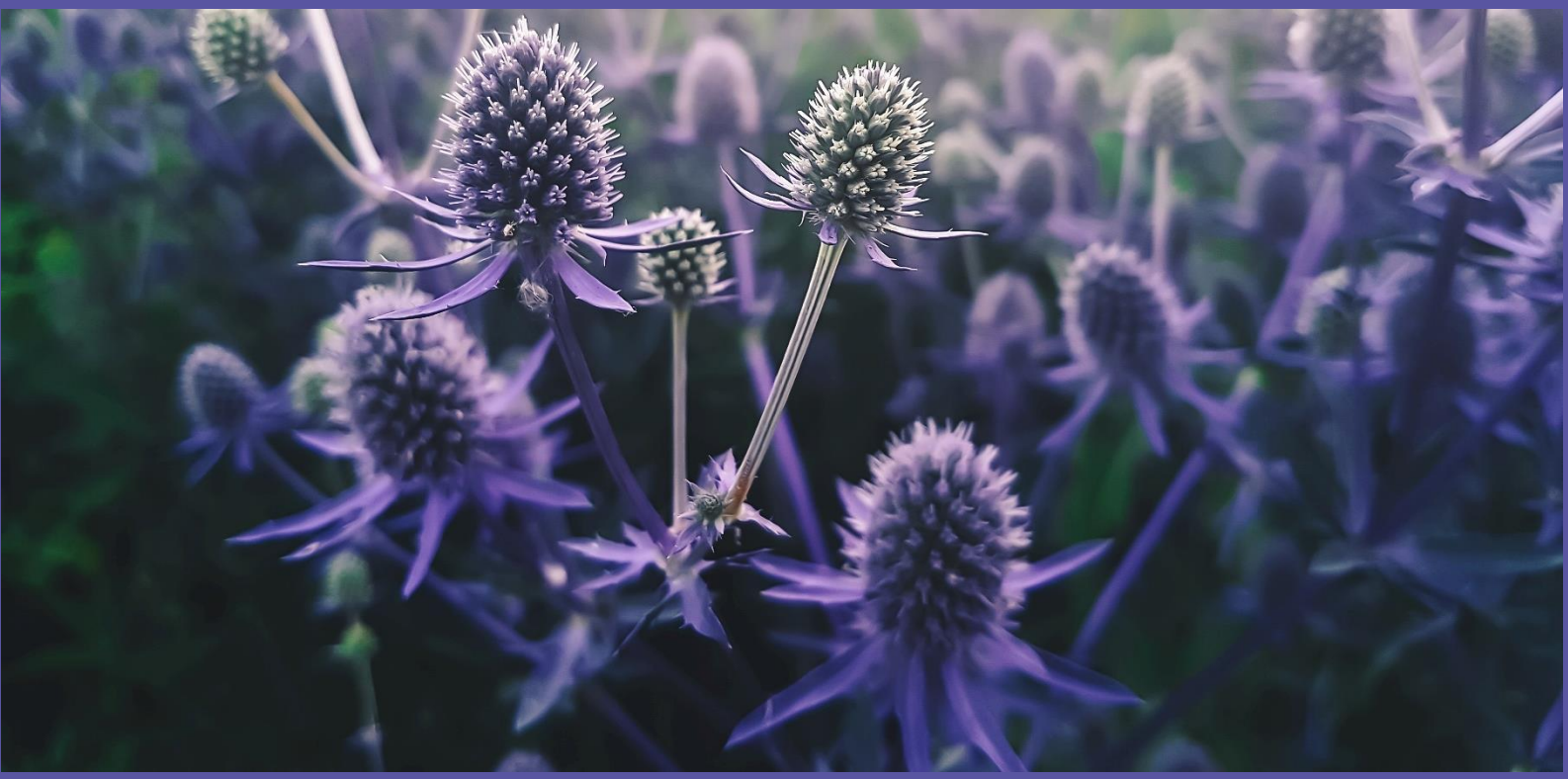
City of Glasgow College

Data Protection

Internal Audit report No: 2022/08

Draft issued: 17 November 2022

Final issued: 22 November 2022



Henderson Loggie

		Page
Section 1	**Management Summary**	
	• Overall Report Grade	1
	• Risk Assessment	1
	• Background	1
	• Scope and Objectives	2
	• Audit Approach	2
	• Summary of Main Findings	3
	• Acknowledgements	3
Section 2	**Main Findings and Action Plan**	**4 - 7**

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 and 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

Satisfactory	System meets control objectives with some weaknesses present.

Risk Assessment

This review focused on the controls in place to mitigate the following risks on the City of Glasgow College Risk Register:

- Information and IT - Failure of Compliance with the General Data Protection Regulations
- Information and IT - Non-Compliance with Freedom Of Information Legislation

Background

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'.

As part of the Internal Audit programme at City of Glasgow College for 2021/22 we carried out a review of the college's implementation of the Data Protection Act 2018, including the UK GDPR, to ensure that processes and procedures are in place to allow compliance with this.

Within City of Glasgow College, the oversight for managing the college's compliance with data protection legislation and regulations sits with the Depute Principal and Chief Operating Officer. Assisting them with this is an outsourced Data Protection Officer (DPO) working on a flexible contract of 3 days per week, who applies their professional expertise in the development of key data protection controls within the college's data protection framework. This includes managing data breaches, assisting with subject access requests (SARs), training and development, and aligning the college's data protection framework with the Information Commissioner's Office (ICO) Framework.

The processes in place for ensuring compliance with data protection legislation and regulations are defined by a Data Protection Policy, Data Protection Breach Procedure, Data Protection Privacy Notices (for students, staff and Board members) and other key procedural documents which are available to all college staff via the intranet. Additionally, the college's Data Protection Policy, Data Breach Procedure and Privacy Notices are publicly available on the college website, and provide key information such as: the organisation's lawful basis for processing data, the nature of the data which it collects, the rights of its data subjects and further contact information should the user require it.

Scope, Objectives and Overall Findings

The Data Protection Act 2018 (DPA) sets out the framework for data protection law in the UK. It updates and replaces 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. We carried out a review of the work carried out to ensure ongoing consistent application of the DPA and GDPR principles across the organisation.

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

Objective	Findings			
The objective of our audit was to ensure that:		**1**	**2**	**3**
		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.	**Satisfactory**	-	-	1
2. Adequate procedures are in place for the ongoing monitoring of compliance with data protection legislation.	**Satisfactory**	-	-	1
Overall Level of Assurance	**Satisfactory**	**-**	**-**	**2**
		System meets control objectives with some weaknesses present.		

Audit Approach

Through discussions with the Depute Principal and Chief Operating Officer and the College's Data Protection Officer, the actions taken to date by the College were established, in addition to any further actions planned, to implement the requirements of the Data Protection Act 2018, including the requirements of the UK GDPR. The Information Commissioner's Office guidance was be used as the basis for this discussion, and any additional actions required have been highlighted.

Summary of Main Findings

Strengths

- A Data Protection Policy in place which is publicly accessible via the College's website;
- The appointment of an external DPO allows the College to meet the ICO requirement for the DPO to be "*independent and unbiased. They must report to the highest management level, and staff must be clear about how to contact them*";
- The DPO has undertaken a gap analysis of the College's compliance with the ICO Framework and scheduled actions to address any shortcomings;
- Separate privacy notices are in place for staff, students and Board members to allow role specific information to be provided;
- A detailed Data Breach Procedure document is in place, and this is available to all College staff;
- There is a direct, secure, data breach reporting facility in place, which is available to all College staff;
- A Data Privacy Impact Assessment template is in place for use by all staff who require it;
- Professional advice is sought from the Data Protection Officer by College staff on subject access requests to ensure that they are handled appropriately and in line with the regulatory requirements;
- The College's contract with the DPO is designed to allow the DPO to provide a flexible service to the College, and therefore allows the DPO to promptly address any issues which require immediate attention;
- The DPO consults regularly with operational management regarding data protection compliance matters; and
- Training has been delivered to College staff on handling data breaches, managing SARs, data protection within procurement, awareness of how to safely share data and data protection due diligence.

Weakness

- Reporting of progress updates for the College's data protection framework is currently in place to the Audit & Assurance Committee. However, no regular reporting is in place on data protection to the College Board; and
- As a result of the record of processing activities (ROPA) being incomplete, no periodic compliance checks are in place to ensure that personal data is being retained in line with regulatory requirements.

Acknowledgment

We would like to take this opportunity to thank the staff at City of Glasgow College who helped us during the course of our audit.

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.

The College has a DPO in place, who is externally contracted from the legal firm Thorntons. The contract is specifically held with the Director of Data Protection at Thorntons, with work also performed by another Solicitor who reports to them, who is a Certified Specialist in Data Protection. The contract is for three days per week, with the specific days varying from week to week, depending on schedules and meeting requirements. The DPO retains responsibility for maintaining all Policy and procedural documents, in relation to data protection, as part of the contract in place, in addition to managing subject access requests.

The DPO also manages a mailbox for data breaches, which allows users to provide breach information to the DPO for their assessment to establish any remediation required and in particular, any breaches which may require to be reported to the Information Commissioner's Office (ICO). A schedule of the breaches is maintained by the DPO as evidence to ensure that all breaches are logged, and their actions recorded to comply with the Data Protection regulations.
From our review of the documentation, the Data Protection Policy was last updated in 2021 to reflect changes brought about by the UK departure from the EU, with the next review scheduled for 2023. The ownership of the Data Protection Policy rests with the DPO.

The Data Protection Policy includes key areas including:

- Details of the legislation / regulations which define the procedures;
- The college's roles and responsibilities under these laws and regulations;
- Whose data is affected by the College;
- The fair and lawful processing of data;
- Information relating to data subjects;
- Data protection and retention;
- Roles of specific key personnel;
- Related procedural documents; and
- Document control arrangements.

From our review of the College's Data Protection Policy, it was established that the key roles for the College (and its personnel) are formally defined, with relevant procedural documents in place to monitor compliance.

There is a Privacy Notice in place for employees (issued in March 2018), students and Board members, which provides the reader with key information regarding how their data is collected, shared, processed, managed and retained. This provides the reader with an understanding of the College's responsibilities regarding data protection.

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

Observation	Risk	Recommendation	Management Response
Reporting on progress in developing the College's data protection framework is currently in place with updates provided to the Audit and Assurance Committee. However, there is currently no regular reporting on data protection matters to the College Board. Given the risks which data protection compliance presents to the College, and the fact that the DPO is in the process of implementing a data protection framework within the College to ensure ongoing compliance, it is our view that the Board should be made aware of any significant control changes and any changes to the data protection landscape within the College.	There is a risk that the Board is not adequately aware of data protection issues and developments within the College.	**R1 –** It is recommended that periodic reporting to the Board be implemented to inform the Board of progress on the implementation of the data protection framework within the College, as well as any significant data protection issues and reportable breaches.	Agreed. The College recognises that it would be beneficial to extend data protection reporting to the Board to ensure that awareness of risk and assurance activity is delivered to the highest level of management. We will add the data protection report to the College Board agenda to be delivered quarterly. **To be actioned by:** Depute Principal with DPO **No later than:** From Board Meeting of 12 December 2022
			Grade **3**

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

Data Breaches

There is a designated mailbox in place, which allows College staff to submit queries regarding data protection issues and to report potential breaches. The staff member responsible for the breach completes a data breach report. The data breach form is available via the College intranet and is designed to capture the nature of the breach. The DPO then reviews the breach and recommends corrective actions, where relevant, and assesses whether the breach is reportable to the ICO. The DPO then logs the details of the breach on the data breach register and retains a copy of the forms as evidence. Details of any breaches received in the academic year are reported in an update provided to the Audit and Assurance Committee, with additional context provided on any breaches reported to the ICO.

Subject Access Requests

Subject Access Requests (SARs) are commonly submitted to Student Records / Human Resources teams as they often relate to staff or student records. Additionally, the College also receives requests from sponsors and employers who require information on student performance and / or any information on issues on their student record which the student may / may not have voluntarily disclosed. Additional requests for data are also received from the public, Police Scotland and Student Awards Agency Scotland (SAAS). Upon receipt of a request, the process owner contacts the DPO, who then consults with the member of staff who retains the data and actively works with them to fulfil the request, where possible, by providing the requestor with the relevant information, and redacting any irrelevant private information.

Compliance Spot Checks

The spot check process is still under development as the DPO is in the process of completing a record of processing activities (ROPA) for all areas of the College. Once this work has been completed, with a projected completion date of the final quarter of 2022, a spot check process will be possible as the information regarding the types of data held by each department will provide the DPO with a baseline position, which the DPO can conduct checks against.

Management Reporting

The DPO has developed a tailored approach to ensure that the College is aligned to the ICO Framework. The DPO has performed a gap analysis to ensure the College has a complete framework of its own. In order to achieve this, the DPO has worked across all departments and faculties on a risk basis, focusing on HR, International Development and Partnerships, and other data heavy data processors. Quarterly reporting to the Depute Principal and Chief Operating Officer is in place to provide regular updates on their progress,

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

Observation	Risk	Recommendation	Management Response
As a result of the DPO's ongoing work to finalise the record of processing activities (ROPA) within the College, there is currently no periodic spot checks of data retention practices within the College to help ensure that data processors are holding data in line with the defined retention periods.	There is a risk that instances of data being held out with the requirements of data protection legislation and regulation may not be detected in the absence of spot checks being carried out.	**R2 –** It is recommended that the ROPA be finalised and agreed by the DPO. It is also recommended that upon completion of the ROPA, the DPO implement a schedule of periodic spot checks for data retention practices with the relevant data processors.	Agreed. The College acknowledges the gap in our record of processing activity, which is being proactively addressed and progressed by the DPO. Progress is being made in the completion of the ROPA with ongoing monitoring of the finalised record of processing activity a priority. As soon as the ROPAs for all areas of the College have been completed, a schedule of periodic spot checks will be implemented. **To be actioned by:** Depute Principal with DPO **No later than:** ROPA complete for whole College and spot checking introduced by the end of February 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