Item 08b

LEVEL OF ASSURANCE
Good

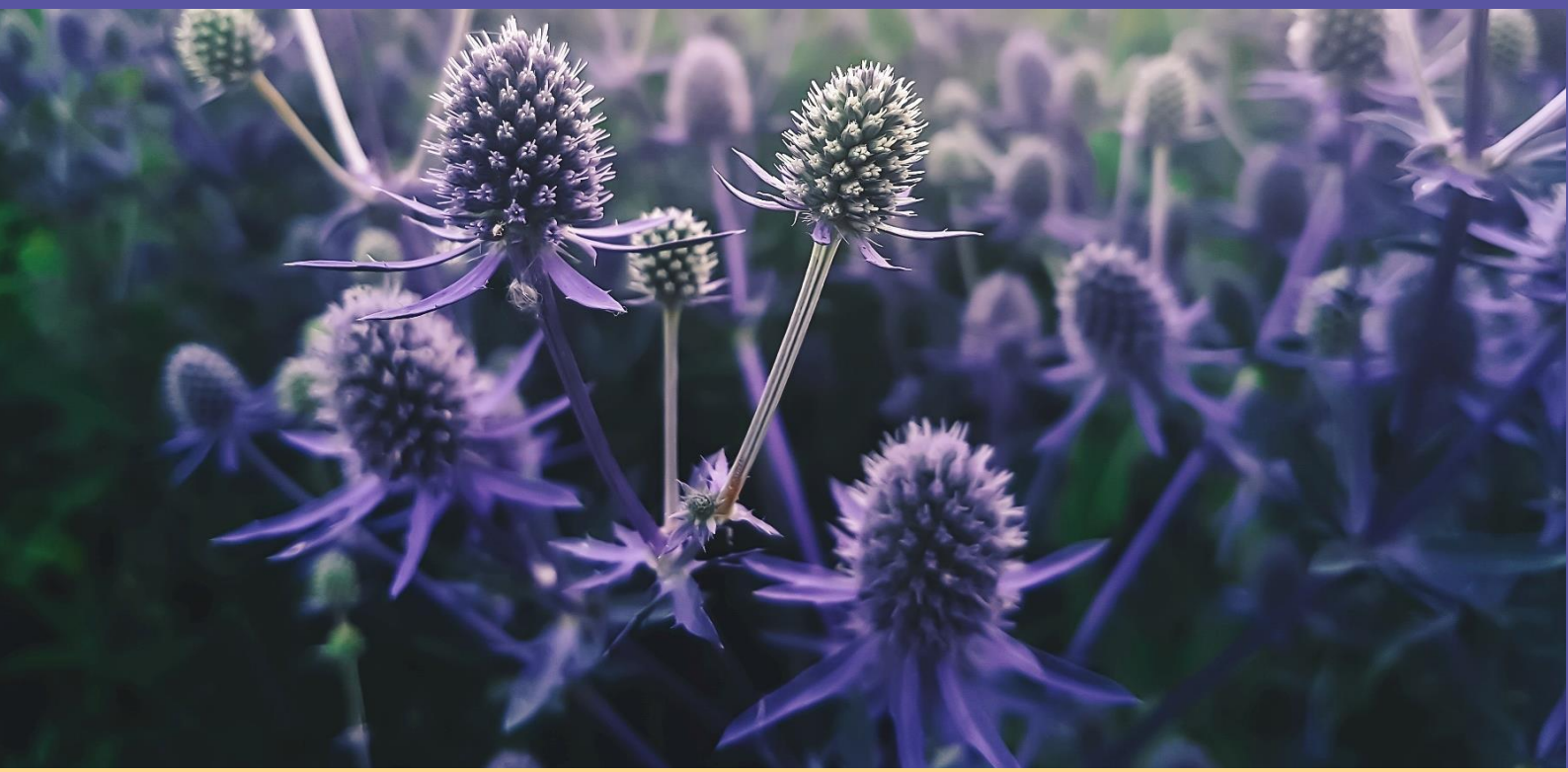
Glasgow Kelvin College

Data Protection

Internal Audit report No: 2022/04

Draft issued: 9 May 2022

Final issued: 10 May 2022



Henderson Loggie

Contents

		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**	**4 - 6**

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 Risk 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 Glasgow Kelvin College ('the College') Strategic Risk Register:

Serious breach of legislation, including:

- Health & Safety
- Charities
- GDPR and Data Security
- Intellectual Property and Copyright
- Environmental Health
- Public Procurement Regulations and legislation
- Equality Legislation

This would have financial consequences (fines) and result in severe reputational damage (risk rating: green)

Background

As part of the Internal Audit programme at the College for 2021/22, we carried out a review of the organisation's data protection arrangements. Our Audit Needs Assessment identified this as an area where risk can arise and where Internal Audit can assist in providing assurances to the Principal and the Audit and Risk Committee 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.

Scope, Objectives and Overall Findings

The audit included a review of the work carried out to ensure ongoing and consistent application of the DPA and GDPR principles across the organisation.

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

Objective	Findings			
To obtain reasonable assurance that:		**1**	**2**	**3**
		No. of Agreed Actions		
1. Appropriate action has been taken by the College to assess compliance with data protection legislation through a self-evaluation exercise which assesses the strength of the data protection framework developed and the extent to which this framework has been in embedded within operational processes.	**Good**	-	-	-
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.	**Good**	-	-	-
Overall Level of Assurance	**Good**	**-**	**-**	**-**
		System meets control objectives.		

Audit Approach

Through discussion with the Director of Corporate Services and the Data Protection Officer we established the action taken to date by the College and any further action planned, to assess compliance with data protection legislation, including the self-evaluation activity carried out to establish the extent to which the requirements of the legislation have been embedded across the organisation. We then tested the conclusions drawn on the extent to which the data protection framework has been embedded across the organisation through review of key documents and compliance evidence.

We also examined the extent to which robust monitoring arrangements have been built into the data protection framework with a view to confirming whether the existing arrangements are sufficiently mature to allow robust reporting on ongoing data protection compliance to both the senior management team and to the Audit and Risk Committee going forward.

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, information asset register, data breach and Subject Access Request reporting monitoring arrangements; a privacy network comprising data protection champions; and mechanisms for identifying and assessing data protection risks.
- An internal data protection team is in place with a College appointed Regulations and Compliance Manager responsible for all operational aspects of data protection (who is supported by an external DPO accessed through HEFESTIS); and
- Governance structures are in place to maintain oversight of data protection compliance across the organisation and these arrangements are working effectively.

Weaknesses

No significant weaknesses were identified during our review.

Acknowledgment

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

Main Findings

Objective 1: Appropriate action has been taken by the College to assess compliance with data protection legislation through a self-evaluation exercise which assesses the strength of the data protection framework developed and the extent to which this framework has been in embedded within operational processes.

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 data protection legislation. We reviewed key policies and procedures, and we also met with the Director of Corporate Services and the Data Protection Officer (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 HEFESTIS (HE/FE Shared Technology & Information Services) 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) 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.
- 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. Review of compliance statistics noted a high level of staff (80%) have completed the mandatory training. 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 assess compliance with data protection legislation through a self-evaluation exercise which assesses the strength of the data protection framework developed and the extent to which this framework has been in embedded within operational processes (continued).

- A Data Protection team has been established within the wider Corporate Services Department, which oversees the development and implementation of data protection procedures. The Data Protection team is supported by an external Data Protection Officer (DPO), through its subscription to HEFESTIS, for one day per week. 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 Data Protection team is further supported by a network of data protection champions through the Privacy Network which assists in providing oversight of data protection matters, including compliance arrangements, and cascading training and relevant data protection updates to their teams.
- Data Protection Impact Assessments (DPIAs) have been undertaken as part of the implementation of new 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 College data protection team, including data gathering, reviewing, and redacting the data and responding to the data subject. However, all SAR responses are processed through the dedicated mailbox and complex or sensitive cases are discussed with the DPO prior to the College issuing a formal response.
- A Data Protection Policy which reflects Information Commissioner's Office (ICO) guidance.
- An overarching Privacy Notice which reflects the range of data protection engagements with staff, students and stakeholders and reflects ICO guidance.
- A Privacy Network which provides a forum for oversight of data protection matters, including compliance arrangements, identifying data protection issues across the College and communication of data protection guidance to staff.
- Regular reporting of data protection issues as they arise to the Risk Management Committee (which is an internal management group), the Senior Management Team and the Audit and Risk Committee.

In November 2021, the Governance Update reported by the Director of Corporate Services to the Audit and Risk Committee included the results of the College's self-evaluation of the ICO's Accountability Framework, which 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 in the majority of areas, and partially meeting expectations in the few remaining areas, including training and monitoring. Improvement actions have been agreed by the College to address these areas. As part of our audit, we 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 achieving a higher rate of compliance for staff training, although current rates are considered to be high, and producing an annual Data Protection Officer's report for the Audit and Risk Committee (as noted under objective 2).

Based on our review we are, overall, satisfied that the College has sound data protection policies and procedures in place.

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, Data Protection team and the Privacy Network all play a key role in the oversight and application of the College's data protection procedures. The DPO meets regularly with the Director of Corporate Services to discuss relevant issues and challenges. One 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. The Director of Corporate Services participates in the Privacy Network, which has a role in the operational and day-to-day responsibility for monitoring implementation of the College's procedures and therefore compliance with legislation. If required, data protection issues, including any significant instances of non-compliance with procedures or legislation, would be reported to the Risk Management Committee, Senior Management Team, and the Board via the Audit and Risk Management Committee, with any improvement actions also communicated to the staff via the Privacy Network.

High level data protection metrics are reported to the Risk Management Committee during the year which provide an update on the College's performance in complying with its obligations under the data protection legislation. Data protection compliance metrics reported on include the number of SARs and other types of requests made under the legislation, the number of data security incidents reported, and the number of requests made by law enforcement agencies.

In addition to the above reporting, SARs are recorded and monitored by the Data Protection team and detailed metrics in relation to completing SARs within the one-month statutory timescales are monitored by the Director of Corporate Services and the DPO. We noted that there was scope for the existing reporting of metrics to be expanded to include details of SAR responses being completed within statutory timescales, and details of data breaches / security incidents which were reported to the ICO or not. This has been recognised by the College and in future the additional information, along with a summary of key data protection activities, will be reported to the Audit and Risk Committee by way of an annual DPO report. The first annual DPO report is expected to be published later in 2022 after the end of the 2021/22 academic year.

The College has developed an internal GDPR audit plan to monitor compliance with its own policies and procedures and to obtain assurances that business processes are operating in compliance with current legislation. The audit plan includes 'mini audits', conducted by the Data Protection team, which include spot checks of departmental records to ensure compliance with data retention schedules; review and refresh of data protection policies and procedures; training; and provision of advice to staff on how to recognise and respond to SARs and data breaches; review of the RoPA to ensure completeness; and review of Privacy Notices. At the time of our review, three mini-audits had been undertaken across different College departments. In addition, the DPO conducts detailed reviews of business processes, targeting higher risk areas, such as MIS (Management and Information Systems) and Advice, Guidance and Learner Support. The DPO then reports to the Risk on findings along with any remedial actions required.

Based on our review we are, overall, satisfied that the College has good data protection policies and procedures, and therefore an adequate data protection compliance framework is in place.

Henderson Loggie

Aberdeen 45 Queen's Road AB15 4ZN T: 01224 322 100 F: 01224 327 911
Dundee The Vision Building, 20 Greenmarket DD1 4QB T: 01382 200 055 F: 01382 221 240
Edinburgh Ground Floor, 11-15 Thistle Street EH2 1DF T: 0131 226 0200 F: 0131 220 3269
Glasgow 100 West George Street, G2 1PP T: 0141 471 9870

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.