Board of Management:

Audit Committee

Date of Meeting	Wednesday 18 September 2019
Paper No.	AC1-L
Agenda Item	12
Subject of Paper	Internal Audit Data Protection Update
FOISA Status	Disclosable
Primary Contact	Sheila Lodge, Depute Principal
Date of production	August 2019
Action	Discussion

1. Recommendations

The Committee is asked to discuss and note this update on progress towards completing the actions arising from the Internal Audit report on Data Protection, April 2019 (audit no. 2019/02).

Board of Management

Date of Meeting	**28 August 2019**
Paper No.	**BOM1-J**
Agenda Item	**16: AOCB**
Subject of Paper	**Data Protection Audit, April 2019: update**
FOISA Status	**Disclosable**
Primary Contact	**Dr Sheila Lodge**
Date of production	**23 August 2019**
Action	**To note**

1. Recommendations

The Board is asked to note this update on progress towards completing the actions arising from the Internal Audit report on Data Protection, April 2019 (audit no. 2019/02).

2. Purpose of Report

To update the Board on progress to date towards completing the actions arising from the Internal Audit report on Data Protection, April 2019 (audit no. 2019/02).

3. Context and Content

In April 2019, our internal auditors, Henderson Loggie, undertook an audit of Data Protection across the College. The audit report noted that the area 'required improvement'. A management response showed that all recommendations had been accepted, and an action plan was put into place.

The attached version of the Audit report incorporates the management response, the action plan and an update on progress to date towards completing each action.

However, it is regrettable that progress on complying with the recommendations has been delayed by the time taken over the summer to appoint a Data Protection Officer.

Until March 2019, Julia McAfee, Director of Corporate Support, acted as the College's Data Protection Officer. Following her departure, it was decided that the College should employ a dedicated Data Protection Officer for three days a week, and should source this appointment through HEFESTIS, a not-for-profit Shared Service organisation jointly owned by all its member Universities and Colleges across Scotland. HEFESTIS operates alongside Advanced Procurement for Universities and Colleges (APUC), the centre of procurement expertise for Scotland's tertiary sector.

HEFESTIS recently established a new Data Protection Officer (DPO) Shared Service of seven Data Protection Officers to serve a large proportion of their member institutions across Scotland. All roles in the team entail being the named Data Protection Officer for one or more higher or further education institutions and linked bodies within a defined region. These roles form a team of Data Protection Officers which provides a peer network of support and expertise, while providing an effective and resilient resource for client institutions, with cover for any absence. This guarantees the College a higher degree of protection than appointing a stand-alone DPO would have done.

As HEFESTIS did not have the capacity to provide a DPO immediately, they advertised the post and moved to appoint. In the interim, they provided Mairead Wood, an experienced DPO, to advise the College, but only for one day a month. Although she was very helpful and willing to support the College at any time with an urgent issue, she was not in a position to tackle the actions arising from the audit action plan.

Guy Clinton was successfully appointed to be CoGC DPO, and took up the post on 19 August. Unsurprisingly, the long gap from April to August has meant that progress on complying with the audit's recommendations has not been as swift as would have been wished. However, Guy has a wealth of experience as a DPO and a consultant on GDPR (the General Data Protection Regulation), and has made an excellent start to his new role, so there is confidence that progress will now accelerate markedly.

4. Impact and implications

Complying with the recommendations of the audit, and taking further actions beyond compliance, will ensure that the College is fully compliant with all legal requirements and develops a culture of robust data protection. The College now has appropriate staff in post to take this forward.

Appendix:

Internal Audit report on Data Protection, April 2019 (audit no. 2019/02), with management response and update on actions, 23 August 2019.

mha
HENDERSON LOGGIE

City of Glasgow College

Data Protection

Internal Audit Report No: 2019/02

Draft Issued: 22 April 2019

Final Issued:

LEVEL OF ASSURANCE	Requires Improvement

Action Plan Update: 23 August 2019

Content

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 College to material risk and which requires to be brought to the attention of the Audit Committee.
Priority 2	Issue subjecting the College to significant risk and which should be addressed by management.
Priority 3	Matters subjecting the College to minor risk or which, if addressed, will enhance efficiency and effectiveness.

City of Glasgow College
Data Protection DRAFT

mha
HENDERSON LOGGIE

1. Overall Level of Assurance

Requires Improvement	System has weaknesses that could prevent it achieving control objectives.

2. Risk Assessment

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

- Failure of compliance with the General Data Protection Regulations (GDPR) (net risk score: 8); and
- Negative impact of statutory compliance failure (net risk score: 10).

3. Background

As part of the Internal Audit programme at the College for 2018/19 we carried out a review of the College's data protection framework, including compliance checks. The Audit Needs Assessment, completed in March 2017, identified this as an area where risk can arise and where Internal Audit can assist in providing assurances to the Board of Management and the Principal that the related control environment is operating effectively, ensuring risk is maintained at an acceptable level.

GDPR

The Data Protection Act 2018 (the Act), which incorporates the EU General Data Protection Regulation (GDPR), came into force in the UK on 23 May 2018. This legislation included an expanded definition of personal data and a greater number of specific responsibilities now defined as mandatory. Non-compliance with the GDPR may result in significant fines.

To help prepare for GDPR there were 12 steps that the Information Commissioner's Office advised that organisations take. These cover the following areas:

1. Awareness;
2. Accountability;
3. Information you hold;
4. Privacy by design and impact assessments
5. Data Protection Officers
6. Legal basis for processing data
7. Consent;
8. Children;
9. Communicating privacy information;
10. Subject access requests;
11. Data breaches;
12. International

4. Scope, Objectives and Overall Findings

We carried out a high-level review of the College's implementation of the Act, which included checking that there were appropriate processes and procedures in place to ensure compliance with the Act.

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

Objective		Findings			
The objective of this audit was to obtain reasonable assurance that:	**Assurance**	**1**	**2**	**3**	**Actions already planned**
		No. of Agreed Actions			
1. Appropriate action has been taken by the College to put a framework in place to comply with the requirements of the Act	**Requires Improvement**	0	4	1	✓
2. Adequate procedures are in place to monitor compliance with the Act	**Requires Improvement**	0	3	0	✓
Overall Level of Assurance	**Requires Improvement**	**0**	**7**	**1**	
		System has weaknesses that could prevent it achieving control objectives.			

5. Audit Approach

Through discussion with the Director of Corporate Support and other staff, listed below, we established the action taken to date by the College, and any further action planned, to implement the requirements of the Act. The Information Commissioner's Office guidance was used as the basis for this discussion, and any additional action required has been highlighted.

Interviews conducted:

- Director of IT and Head of Digital Services
- Finance Manager
- Head of Organisational Development
- Head of Human Resources
- Curriculum Head for Accounts & Business Services and Senior Lecturer, Accounts & Business Services
- Head of Student Data and Research
- Head of Admissions
- Lead Procurement Manager

6. Summary of Main Findings

Strengths

- The College has developed a framework of data protection documents and complimentary procedures that are easy to locate on the College website. This includes: the Data Protection Policy; Privacy Notices; Document and Records Retention Policy; Data Privacy Impact Assessment; Student Personal Data Guide; Requests for Personal Data Guide; and Data Breach Procedure;
- A wide range of training has been provided to staff to help them understand the Act's requirements; and
- A data map has been produced which sets out the different documents which record personal data and identifies the required retention period and any legal requirements for retention.

Weaknesses

- College staff interviewed were not aware of all of the key requirements of the Act, which highlights the need for ongoing training to address these knowledge gaps;
- Existing procedures have not been updated to introduce the data protection controls required to ensure compliance with the Act;
- The legal basis for holding personal data has not been formally documented;
- There was no process to ensure that personal data held beyond the set retention period was disposed of appropriately. This includes information on software systems, in network drives, in emails and in locations where hard copy documentation was held; and
- There was no data protection compliance framework in place to demonstrate that key data protection requirements were being complied with.

7. Acknowledgements

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

8. Findings and Action Plan

Objective 1: appropriate action has been taken by the College to put a framework in place to comply with the requirements of the Act

We completed the ICO checklist and from this exercise we noted the following against each of the checklist headings:

Information you hold

A data map has been prepared setting out the personal data the College holds using a standard template provided by JISC. This sets out retention periods, the statutory basis for holding data (if it is related to a legislative requirement) and who is responsible for the data. We noted that the College now has a range of data sharing agreements in place. Although there are no data sharing agreements in place with Education Scotland or Skills Development Scotland (SDS) we were advised by the Data Protection Officer that that this is representative of the sector and that this matter is being progressed by the sector Scottish Colleges Information Governance Group.

Data Protection Officer

At the time of audit fieldwork, the College had a Data Protection Officer, however they left the College in March 2019 during our audit review. Until new arrangements come into force. the Depute Principal & Chief Operating Officer is overseeing the area with the assistance of a DPO from HEFESTIS who usually attends the College for 1 day each month, but who will be with us for 3 days a week.

Children

There are a range of procedures in place to obtain parental/guardian permission in the event of an individual under the age of 16 applying for a course. The Schools College Partnership work is arranged between schools and the College (rather than between individual students and the College).

Communicating privacy information

Privacy notices clearly set out what the College will do with individuals' personal data and can be accessed via the College website. The application and enrolment forms also have links to the College's terms and conditions, which include data protection clauses and reference to the student privacy notice.

Data Breaches

There is a data breach procedure and all data breaches identified must have a data breach form completed which sets out any follow-up action required to strengthen controls. A log of all data breaches is also maintained.

International
The College does not operate in more than one EU state, so this is not applicable.

Objective 1: Appropriate action has been taken by the College to put a framework in place to comply with the requirements of the Act

Observation	Risk	Recommendation	Management Response
Awareness We confirmed that there had been a concerted effort to provide training to staff in advance of the 25 May 2018 GDPR implementation date. We obtained a listing of those that received training from the Data Protection Officer, which demonstrated that 226 people had received training. We also obtained records of the staff members who had completed the mandatory online data protection training video between 1 May 2018 and 28 February 2019 and noted that 530 staff had completed this training. Although these are significant numbers of staff trained, they still represent only a proportion of the total staffing complement employed across the College. We were advised by the staff members interviewed that information had also been disseminated by email, or training cascaded to staff by those that had attended the formal data protection training sessions. However, from discussion with a range of staff interviewed as part of this audit it was apparent that not all staff demonstrated a comprehensive understanding of data protection roles, documents and requirements. Furthermore, the Head of Organisational Development advised that there were no plans in place to deliver a programme of refresher data protection training.	Staff may not be sufficiently aware of the requirements of the Act which may lead to inadvertent breaches of the Act.	**R1** Introduce a formal, risk-based training programme for data protection and information security. This should include general refresher training for all staff, with more detailed, tailored training designed for staff in departments that deal with a significant volume of personal data.	This recommendation is accepted. **To be actioned by:** DPO **No later than:** Ongoing, but with a first pass of refresher training completed by December 2019 **Update 23.8.19:** Online refresher training will be designed and rolled out through OD. Tailored face-to-face sessions will be organised for staff in departments that

Deleted:

			handle a significant volume of personal data.	
			Grade	2

Objective 1: Appropriate action has been taken by the College to put a framework in place to comply with the requirements of the Act (Continued)				
Observation	**Risk**	**Recommendation**	**Management Response**	
Accountability There should be appropriate management support and direction for data protection compliance in a framework of policies and procedures. We noted that the College has: • A Data Protection Policy; • Information Security policies that are currently being updated or finalised; • A number of specific data protection procedures, such as those related to breaches or data subject requests; • Data protection requirements should be embedded in existing departmental procedures, but we found that there had not been a comprehensive review of existing procedures to allow the introduction of appropriate data protection controls. During detailed testing we noted a number of areas where procedures were required, or required updating, relating to: identification checks to confirm authority to provide references for ex-staff members; the process to refer staff to the College's occupational therapist; procedures for notifying ICT of changes in staff; and procedures setting out identification checks before the provision of information to third parties (such as parents or partners); • Privacy notices for staff, students and Board members; • An updated CCTV code of practice; • Procurement processes include consideration of data protection for new contracts; and	Without embedding data protection within existing procedures there is a risk that the requirements of the Act will not be fully met.	**R2** Embed data protection within existing procedures or create additional procedures for those areas identified where a new procedure is needed.	This recommendation is accepted. **To be actioned by:** DPO working with the Organisational Effectiveness Manager **No later than:** December 2019 **Update 23.8.19:** DPO now working with Operational Effectiveness Manager.	
			Grade	**2**

- Data protection roles are described clearly within the Data Protection Policy.				

Objective 1: Appropriate action has been taken by the College to put a framework in place to comply with the requirements of the Act (Continued)

Observation	Risk	Recommendation	Management Response	
Privacy by design and impact assessments A Data Privacy Impact Assessment (DPIA) form and associated guidance has been developed. However, from our discussions with a range of staff they were not always aware of the existence of this form, or what the purpose of the form was. The key areas for the use of DPIAs are in areas where there are significant levels of personal data held (such as HR/payroll, the student registry system, and IT developments). We noted that the new HR/payroll system was planned prior to the requirement for a DPIA. The student registry system is largely steady state (and managed by an external software provider). We discussed with the Head of Digital Services the processes which were in place within the IT department to ensure that projects relating to handling of personal data had a DPIA undertaken and confirmed that these were not part of the standard IT project requirements.	Without data protection requirements being considered as an integral part of IT projects there is a risk that the software developed (or the software configuration used) will not fully meet the requirements of the Act.	**R3** IT department project workflows should be updated to incorporate the need to routinely undertake a DPIA.	This recommendation is accepted. **To be actioned by:** IT Director **No later than:** December 2019 **Update 23.8.19:** DPO now advising IT Director and Operational Effectiveness Manager.	
			Grade	2

Objective 1: Appropriate action has been taken by the College to put a framework in place to comply with the requirements of the Act (Continued)

Observation	Risk	Recommendation	Management Response
Lawful basis for processing data AND Consent We note that although the data map sets out the personal data held (and the retention periods) it does not describe what the lawful basis for holding personal data is. We also noted some instances where there is confusion over the lawful basis being used. So, for example, the student application form has a consent statement, but this is not required because this is covered by the lawful basis for entering into a prospective contract. We also noted that there are some College forms where the level of information is gathered appears out of alignment with the purpose stated for gathering the information.	The College may not have a lawful basis for collecting and processing data.	**R4** Document on the data map the lawful basis for the use of personal data. Where consent is the lawful basis then the consent form should be reviewed to ensure that it is adequate. Where legitimate interests is used as a lawful basis then the justification for using this basis should be adequately documented.	This recommendation is accepted. **To be actioned by:** DPO **No later than:** August 2019 **Update 23.8.19:** Progress has been delayed by the time taken to appoint the DPO. He is currently working to update the data map and to develop Article 30 Records. **Revised deadline:** November 2019 Grade 2

Objective 1: Appropriate action has been taken by the College to put a framework in place to comply with the requirements of the Act (Continued)

Observation	Risk	Recommendation	Management Response
Subject Access Requests The College has a procedure on the website setting out the procedure for dealing with subject access requests, but it does not currently stipulate who these requests should be sent to. In addition, we noted that some subject access request responses contained personal data identifying which staff member had completed an attendance register. The Head of Student Data and Research has provided assurances that in future this information will be redacted so no separate recommendation has been raised regarding this point.	It may not be clear to staff or students who to send subject access requests to.	**R5** Amend the Requests for Personal Data Procedure to clearly set out who subject access requests should be sent to.	This recommendation is accepted. **To be actioned by:** Head of Student Records / Director, HR, with Operational Effectiveness Manager **No later than:** July 2019 **Update 23.8.19:** Progress was delayed by the time taken to appoint the DPO. He has created a new mailbox for incoming subject access requests and is working with those named above to amend the Procedure. **Revised deadline:** October 2019

			Grade	3

Objective 2: Adequate procedures are in place to monitor compliance with the Act

As part of this review we met with a range of staff from HR, payroll, IT, Student Records, Student Services (covering admissions and student support funds), Organisational Development, procurement and an academic department. From these discussions, and sample observations of systems, network drives, email folders, and physical storage locations we noted the following:

HR

The users and user roles on the new HR/Payroll system had been set up by a staff member who is no longer employed by the College. We discussed with HR staff what assurance they had that the correct user roles had been set up, and that staff were assigned the correct roles (particularly given that there had been a recent restructuring exercise). We were advised that HR staff were planning to review users and user roles on the new system and as work is planned in this area no separate recommendation has been raised. As noted earlier, we found there was the need to formalise the process for dealing with the external occupational health service, and to put in place a procedure over external reference requests (and ensuring that there was appropriate authorisation to release such data).

A small number of hard copy documents with personal data on (which were past their retention date) were found in cabinets in the HR area. It was noted that these items were held in cabinets that are routinely locked out of normal office hours and during College hours staff should be present at all times so this does mitigate the risk of loss of such documents.

Payroll

No issues were noted relating to the payroll function, although staff agreed that the existing retention periods required to be reviewed to ensure ongoing applicability.

Student Records

We noted that some data lists that had been generated to upload into external organisations' portals, such as SQA, had not been deleted but should have been.

The National Insurance Number is requested on the application and enrolment forms but there is no basis for requiring this except for gas training courses and therefore this information should not be routinely gathered for other courses.

Student Services

We noted that there was consent obtained on the student application form but that this is not required.

Organisational Development, Procurement and Academics

Nothing of concern was noted, but it was noted that procedures in relation to data protection will differ between faculties.

Objective 2: Adequate procedures are in place to monitor compliance with the Act (Continued)

Observation	Risk	Recommendation	Management Response
IT Currently when there is a new staff member their line manager will email HR with a completed IT access request form. HR review these emails, put the information onto a spreadsheet, and then email the spreadsheet to the IT system administration team who set up the required access on Active Directory. This spreadsheet is also used for leavers and changes. We noted that when staff leave the employment of the College that this system should ensure that their Active Directory account is removed, although we were advised this information is not passed on within IT to the Enquirer administrator to remove access rights to Enquirer, which does include personal data. We were advised that the College is seeking to achieve Cyber Essentials accreditation in June 2019.	Staff that leave the College may still have access to personal data through the Enquirer system.	**R6** Amend the processes within IT to ensure that when a staff member leaves the College that as well as being deactivated on Active Directory they are also deactivated on Enquirer.	This recommendation is accepted. **To be actioned by:** IT Director / Head of HR **No later than:** June 2019 **Update 23.8.19:** Progress was delayed by the time taken to appoint the DPO. He is now working with the Directors of IT and HR to develop a comprehensive 'off boarding' procedure for departing staff. **Revised deadline:** November 2019. Grade 2

Objective 2: Adequate procedures are in place to monitor compliance with the Act (Continued)				
Observation	**Risk**	**Recommendation**	**Management Response**	
Compliance Checks The College does not have a framework of formal checks as part of a compliance framework to ensure that staff are complying with the Act. We note that the data map sets out responsible individuals for personal data, but there is a lack of clarity on the checks that these staff should undertake to ensure that the College is compliant with the Act; how these should be recorded; and what upward reporting there should be to provide assurance to senior management and to the Board that the College is complying with the Act. We consider that there would be benefit in having more detailed procedures setting out the compliance responsibilities of staff (including a requirement for staff to identify key risks and controls relating to personal data held in their area and undertaking periodic checks to ensure that these controls are functioning effectively), with the results of checks recorded and routinely reported to the Data Protection Officer to allow the review of any issues and reporting to senior management and to the Audit Committee. This will provide information on the framework of compliance checks in place and give assurance on whether these are functioning effectively. There may also be a role for the Data Protection Officer in undertaking risk-based audits of specific areas of the College, with a focus on areas who handle significant volumes of personal data.	Staff may not be complying with the Act.	**R7** Put in place a robust data protection compliance framework that includes clear responsibilities; recording of compliance checks required; and routine reporting of the results of compliance checks (and any associated issues) to senior management and to the Audit Committee.	This recommendation is accepted. **To be actioned by:** DPO **No later than:** August 2019 **Update 23.8.19:** Progress was delayed by the time taken to appoint the DPO. He advises that, given the extent, size and detail of College operations, this will be an ongoing project over the next year. **Revised deadline**: June 2020	
			Grade	**2**

Objective 2: Adequate procedures are in place to monitor compliance with the Act (Continued)

Observation	Risk	Recommendation	Management Response
Deletion The deletion of data once it is past its retention period is an issue in most organisations due to the difficulties in isolating such data. Many organisations are seeking to deploy technological solutions to identify items which require to be deleted, with a view to initiating a process of automated deletion. This includes emails, network folders and software. We noted that the College has no formal process to identify and delete information which has gone past the set retention dates.	Data is retained beyond the set retention date, in contravention of the Act.	**R8** Consider solutions to delete personal data or anonymise this information once it goes past the agreed retention date.	This recommendation is accepted. **To be actioned by:** DPO with Operational Effectiveness Manager **No later than:** December 2019 **Update 23.8.19:** DPO advises extending the remit to ensure use of the right 'privacy treatment' (of which anonymisation might be one option) at the right time in each context. **Revised deadline:** March 2020 **Grade** 2