Board of Management

Date of Meeting	**Wednesday 4 December 2019**
Paper No.	**BoM3-F**
Agenda Item	**5.1**
Subject of Paper	**Internal Audit of Data Protection/GDPR Update**
FOISA Status	**Disclosable**
Primary Contact	**Dr Sheila Lodge**
Date of production	**5 November 2019**
Action	**For Noting**

1. Recommendations

To note the report which was submitted at the last meeting of the Audit Committee on 13 November 2019.

Board of Management
Audit Committee

Date of Meeting	**Wednesday 13 November 2019**
Paper No.	**AC2-F**
Agenda Item	**5.4**
Subject of Paper	**Data Protection Update**
FOISA Status	**Disclosable**
Primary Contact	**Dr Sheila Lodge**
Date of production	**05 November 2019**
Action	**For Noting**

1. Recommendations

The Committee is asked to note this paper.

2. Purpose of Report

This report seeks to update the Committee on progress and achievements to date in relation to the College's data protection arrangements, and sets future milestones and dates for their achievements.

3. Context and content

3.1 The College's new Data Protection Officer (DPO), Guy Clinton, took up his post on 20 August 2019, and has been engaged since then in assessing the College's compliance with data protection legislation, creating the required documentation, developing a network of 'Heads of Privacy' and rolling out training for staff.

3.2 Initial actions

An initial gap analysis of data repositories in most departments has been carried out by the DPO. This identified the following areas that required immediate re-enforcement:

Data Protection Item	**Action Taken**	**Completion status**
Procurement contracts	Updated to reflect correct responsibilities for 3rd Party Processors.	Completed.
Procurement processes for 3rd Party vendors	Updated and fully imbedded for GDPR compliance with an up to date Data Processing Agreement.	Completed.
Police request form for student data	Updated & Implemented for lawful use.	Completed.
Data Sharing Agreement	Improved DSA.	Implemented with on-going use by College when required, incrementally.
Data Protection Impact Assessment	Upgraded to define risk against impact mathematically, and	Implemented document in IT, training still to be done.

	remove some of the objectivity.	
Data Breach Matrix	Implemented with IT.	Designed and written by the DPO this has been sent to the IT Director, the Lead Investigative Officer (for breaches) and the Depute Principal so that, should the DPO be absent, they can precisely and correctly specify the level of risk in a breach, which then determines the legal steps and actions required.
Privacy Notices – Staff and Student	Upgraded to facilitate lawful data usage for UKVI data processing, MP3 and MP4 files.	Completed and posted on the website.
Privacy policies.	These policies are being reviewed and revised by the DPO to reflect minor changes in names of staff and contact points with additional minor changes to reflect all the data protection legislation, not just the DPA 2018.	Target date for posting all of these revisions is end of November 2019.
Data retention schedules.	Currently under review.	They will be finalised and more accurately defined as part of the Article 30 project by end of January 2020; ready for implementation in mid-February.

Lawful basis identification for each type of data processing	Most types identified, with the remainder finalised by the Article 30 project.	Currently 33% complete, to be finalised by end of year.
Subject Access requests	Personal data procedure being updated.	Target date for completion mid-November.
Onboarding & Offboarding processes and automation	Partial completion with improvements and automation planned.	Target date for completion – yet to be agreed with IT department.
HR employment contracts	Updated.	Completed.

3.3 Article 30 (Combination) Project

The aim of this project is to facilitate data privacy Article 30 document population across the College by the end of 2019, while also providing (in the same process) GDPR training in each department, with additional training, knowledge and responsibilities for each nominated Head of Privacy (HOP). HOPs will in turn provide a strong, manageable platform for the turnkey implementation of 80% of full data governance by mid-February.

3.3.1 Historical (unstructured) data

Given

1) the amount of historical data sitting on the network (built up over 15 years +);
2) the current level of training in each department; and
3) the amount of time and resource available in each department to correctly identify the data / data set that could/should be deleted,

there is a need to delete historical data (obsolete/redundant data), and it is planned to undertake this during mid-February as one exercise over a short period e.g. (3- 6 weeks). This will help us meet three of the seven principles of GDPR lawful processing and ‘best practice’ data governance, which are: data minimisation, purpose limitation and storage limitation for holding data. This is, additionally, stated on our Privacy Notices.

3.3.2 Deletion

However, there is a possibility that many departments could 'accidently' delete data that ought to be kept. As accidental loss constitutes a breach under GDPR, the volume of this accidental loss being recorded/reported over a short period could attract unwelcome interest, an enquiry and / or even an audit by the Information Commissioner's Office, which would place unwanted pressure on internal resources. While the prospect of this is low (5-10 % likelihood), the risk is that the accidental deletion of data that staff or students expect to be kept would be difficult for the College. This in turn could trigger a complaint, or a series of complaints - a number of which are more likely to trigger closer scrutiny by the ICO.

The solution to this can be easily managed, by:

1) phasing the deletions over a long / longer period of time, having identified the lowest risk categories of data to delete first (not best practice); or

2) setting up secondary storage where each department initially archives the data, rather than deletes it. It could then be deleted in several years' time.

The latter solution has two options, namely:

1) providing portable hard drives into which the redundant data are archived by each department/user/lecturer etc. For best practice these would be encrypted drives held under lock and key in a separate room / cupboard under (IT) management control;

2) centralised control: IT could set up an automated, separate storage facility that records the data sent to the secondary repository - referenced by department, date, subject etc., but a brief investigation has determined this would need additional temporary IT resources to effect.

These options will be considered by SMT and a plan finalised before Christmas.

3.3.3 Structured data retention (databases)

This project has been identified as having a lower priority and plans will be developed early in 2020.

3.4 Consent Form Project

3.4.1 Consent forms are used in volume by several departments in the College but the current medium used is paper and there were no 'withdrawal of consent' forms. Allowance for the greater use of consent forms may become necessary when we Brexit (if the UK becomes a 'Third Country' as current EU legislation stipulates).

3.4.2 The project to create several alternative consent forms (and their associated withdrawal of consent forms) has been identified and sanctioned with resources allocated. Currently it is at the analysis stage. For ease of set up, speed and lowest cost implementation it is likely these forms will be held, accessed and managed through the website or a sub-domain.

The target date for completion of this project is the end of February 2020.

3.5 Staff training in data protection

3.5.1 Understanding of data protection principles and processes across the College, is at best, patchy, while understanding of the underpinning legislation is negligible. This is partly because the mandatory e-learning module need to be updated and extended to provide more detail. A series of new learning modules has been agreed for completion by end of January 2020.

3.5.2 The content will be written by the DPO and provided to Learning Technologies and Organisational Development for e-learning module production. The first will be a general data protection module and the second will target the correct usage of core software platforms to drive rigour into data input and sharing. Further modules will be identified and produced as required. They will all have a Q&A aspect to support learning.

3.6 The DPO has been working through the recommendations of the Data Protection Internal Audit, to ensure these are all implemented in good time. Appendix 1 provides an update on progress with this.

4. Impact and implications

Complying with the recommendations of the audit, and taking further actions towards compliance, will ensure that the College is compliant with all legal requirements and will support more robust data protection. The College now has appropriate staff in place and responsibilities are structured in a way that provides senior management with both granular and wide-ranging data governance, optimised to a high degree of efficiency, so we can manage both historical data and future best practice management of data.

Appendix:

1. **Update on progress against Internal Audit recommendations.**

Appendix I - Updated Action Plan: Internal Audit Report 2019/02 – Data Protection

Recommendation	Grade	Original Management Comments	To Be Actioned By	No Later Than	Progress at August 2019
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.	2	This recommendation is accepted.	DPO	Ongoing, but with a first pass of refresher training completed by December 2019	The College's previous DPO left the College in March 2019 and their replacement did not commence until 19 August 2019, and they work on a part-time basis. Due to this gap there has yet to be introduced a formal, risk-based training programme for data protection and information security however the new DPO plans to do this. ***Not Yet Past Completion Date*** **As per Guy Clinton 25/9/19** 31/10/19 New Training modules have been authorised by Sheila Lodge as mandatory courses. One general GDPR course for all staff with several other modules specific for lecturers and staff using college systems are currently being written by DPO for roll out before end January 2020.

Recommendation	Grade	Original Management Comments	To Be Actioned By	No Later Than	Progress at August 2019
R2 Embed data protection within existing procedures or create additional procedures for those areas identified where a new procedure is needed.	2	This recommendation is accepted.	DPO working with the Organisational Effectiveness Manager	December 2019	The DPO is working with each department to create documentation for compliance with Article 30 of the GDPR. This will help train staff and will set out the data processing that is being done within departments. ***Not Yet Past Completion Date*** **As per Guy Clinton 25/9/19** **31/10/19 Work in progress 33% completed.** The work on compliance, departmental procedures, policy document upgrades, data privacy training and full data governance will all be achieved through the Article 30 project that is 1/3 complete; with 80% of full data governance achieved by March 2020; working closely with Eleanor Doull on process identification and implementation.

Recommendation	Grade	Original Management Comments	To Be Actioned By	No Later Than	Progress at August 2019
R3 IT department project workflows should be updated to incorporate the need to routinely undertake a DPIA	3	This recommendation is accepted.	IT Director	March 2020	***Work in progress*** ***PBC B Ashcroft*** 31/10/19 DPO edit- **New upgraded DPIA that depicts risk mathematically has been finalised for the College and sent to IT department – training in use to be provided to key IT staff. DPIA to be posted for use by other departments once the training module is complete**.

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.	2	This recommendation is accepted.	DPO	August 2019	This is still being worked on by the new DPO. ***Partially Implemented*** **Revised Completion Date:** 31 January 2020. **DPO 31/10/19** **Data map not found.** **Article 30 document has been widened to include identification of each lawful basis (LB) (and support data governance with training) by processing activity. This project includes the above and also Article 6 b, c & e where appropriate. A Consent project across the college is at the design stage, for automation and compliant usage of Consent, including automated processing of withdrawal of consent forms.** Target date for full project completion (not consent

Recommendation	Grade	Original Management Comments	To Be Actioned By	No Later Than	Progress at August 2019
					project) is end of February 2020.
R5 Amend the Requests for Personal Data Procedure to clearly set out who subject access requests should be sent to.	3	This recommendation is accepted.	Head of Student Records / Director, HR, with Operational Effectiveness Manager	July 2019	The Requests for Personal Data Procedure has been amended to clearly set out who subject access requests should be sent to. ***Fully Implemented*** ***PBC L Anderson***
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. D	2	This recommendation is accepted.	IT Director / Head of HR	June 2019	The Head of IT confirmed that by removing Active Directory Access that Enquirer access is disabled. ***Fully Implemented*** ***PBC B Ashcroft***

Recommendation	Grade	Original Management Comments	To Be Actioned By	No Later Than	Progress at August 2019
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.	2	This recommendation is accepted.	DPO	August 2019	The DPO has a plan to implement full data governance department by department. ***Little or No Progress Made*** **As per Guy Clinton 25/9/19** **Revised Completion Date:** 31 March 2020 31/10/19 1/3 of the way through Article 30 project to achieve 80% of full data governance by end of March 2020 (providing R8 is supported by the Board). Once completed this will identify all items necessary for document compliance .

Recommendation	Grade	Original Management Comments	To Be Actioned By	No Later Than	Progress at August 2019
R8 Consider solutions to delete personal data or anonymise this information once it goes past the agreed retention date.	2	This recommendation is accepted.	DPO with Operational Effectiveness Manager	December 2019	**DPO edit - 31/10/19 One of several technical solutions for archiving historical data needs to be confirmed by SMT, together with robust organisational methods put in place by mid-February 2020 so each Department's Head of Privacy (person) (HOP) can archive their data *prior* to final erasure at a later date (to effect compliance). See accompanying document for details.**