Board of Management

Date of Meeting	**Wednesday 6 June 2018**
Paper No.	**BoM6-K**
Agenda Item	**15**
Subject of Paper	**General Data Protection Regulations (GDPR) Update**
FOISA Status	**Disclosable**
Primary Contact	**Julia Henderson, Director of Corporate Support**
Date of production	**31 May 2018**
Action	**For Noting**

1. Recommendations

Board notes the work undertaken in preparation for the commencement of new data protection laws on 25 May 2018.

It is suggested that the Audit Committee is the appropriate committee for ongoing oversight of the management of data protection and that this is made explicit in their terms of reference.

2. Purpose of report

The purpose of this report is to provide an update to the Board in relation to implementation of key compliance requirements by 25 May 2018, and to set out our plan for improving college compliance beyond that date.

This report does not restate the law and the key changes and implications, which was covered in detail in a report to the Audit Committee on 13 September 2017. A progress report on implementation was considered and discussed in full at the Performance, Remuneration and Nominations Committee on 23 April 2018, the new Data Protection Policy was approved by Audit Committee on 16 May 2018 and an amended risk management action plan for data protection was submitted to that Committee.

3. Strategic Context

Data Protection is now very much a 'whole organisation issue' and can no longer simply be written off as just an IT or legal issue. Clear guidance from the Institute of Governance states that 'decision-makers at the highest levels will need clear, reliable updates from those more closely involved in the management of data throughout the organisation'. This has been achieved to date through the Committee reporting narrated at paragraph 2. It is suggested that the Audit Committee is the appropriate committee for ongoing oversight of the management of data protection and that this is made explicit in their terms of reference.

The Brexit question

UK organisations handling personal data still need to comply with the GDPR, regardless of Brexit. A new UK Data Protection Act came into force on 25th May 2018.

Discussion

GDPR Readiness

A significant amount of work has been undertaken t to ensure that we achieve compliance with the core requirements identified by the Information Commissioner's Office (ICO) in their 12 steps – Preparing for the GDPR. We now have in place all key legal notices, policies and procedures and have taken a range of steps to achieve compliance across the College including:

- New student and staff privacy notices, including a short easy read notice for students and an information animation are all available on our website at this link https://www.cityofglasgowcollege.ac.uk/about-us/data-protection. Our privacy notices have been used by colleagues in other colleges, as examples of good practice;

- New staff procedures for information requests and data breaches;

- Amendment of key contracts where personal data is shared and/or processed by 3rd party contractors;

- Notification of opt in in relation to marketing of our College services (e.g. Amethyst Salon and Beauty, Scholars', City Market);

Our readiness has been internally audited and our internal auditors reported at the last Audit Committee meeting that they were satisfied, at that time, with our progress to achieve compliance.

Raising awareness and training

A key requirement of the ICO 12 Steps is the raising of awareness and training of all relevant staff in data protection. In terms of risk management this goes a long way to demonstrating to the ICO that an organisation has taken the new legislation seriously in the event of a breach event. The Director of Corporate Support has delivered training to over 200 staff and more training is scheduled to take place. All managers were briefed on the new law and the implications for the College on 24th May 2018. An online animation training tool has been written in house and is now mandatory training for all staff.

Broader Recommendations – Information Security and Data Management

We carried out an awareness and information gathering audit exercise internally. During the course of this exercise a large number of staff provided feedback on existing systems and processes and often raised concerns or opportunities for improvement. As a consequence a series of recommendations was made, where gaps or opportunities for improvement were identified.

These recommendations set a basis for a plan to improve compliance beyond 25 May 2018 and to reduce the risk of non-compliance for the College. These recommendations will be reviewed and prioritised for action by the relevant business areas; some can be taken forward within existing operational plans or project work streams and others may require discrete projects.

The internal auditor recommended that a core group oversee the implementation of recommendations which underpin data protection compliance and ongoing compliance. A group composed of key senior data owners has been identified, will be overseen by the Deputy Principal and is scheduled to meet on 26 June 2018.

4. Impact and implications

There will be budgetary implications dependent upon decisions taken in relation to the recommendations report, which may lead to changes to IT systems and development of new college wide processes.

Where we fail to comply there are clear reputational and financial risks for the College both with external stakeholders and with our staff and students. The new law introduces more significant organisational fines, the responsibilities for us as a College, managing personal data, are more onerous and the rights of individuals in relation to their personal data are strengthened.

There are opportunities to reduce our risk exposure significantly by addressing key recommendations arising from the awareness and information gathering exercise.