# Board of Management

# Audit Committee

| | |
|---|---|
| **Date of Meeting** | **Wednesday 13 September 2017** |
| **Paper No.** | **AC1-L** |
| **Agenda Item** | **11** |
| **Subject of Paper** | **General Data Protection Regulations (GDPR)** |
| **FOISA Status** | **Disclosable** |
| **Primary Contact** | **Julia Henderson, Director of Corporate Support** |
| **Date of production** | **August 2017** |
| **Action** | **For Noting** |

**Recommendations**

The Committee is asked to note the GDPR paper which was considered and approved by SMT on 9 August 2017.

# Senior Management Team

| | |
|---|---|
| **Date of Meeting** | **9 August 2017** |
| **Paper No.** | **SMT 01-B** |
| **Agenda Item** | **3** |
| **Subject of Paper** | **The General Data Protection Regulations (GDPR)** |
| **FOISA Status** | **Disclosable** |
| **Primary Contact** | **Julia Henderson, Director of Corporate Support** |
| **Date of production** | **3 August 2017** |
| **Action** | **For Approval** |

**Recommendations**

- To seek SMT approval to establish a GDPR implementation project with ELT sponsorship to ensure that the College is well prepared for GDPR commencement on 25 May 2018.
- Suggested initial membership is proposed to include:
  Fares Samara, Stuart Thompson, Julia Henderson, Gillian Plunkett, Jo Maguire (or nominee), Louise Anderson and ICT nominee.

## 1. Purpose of Report

To raise awareness amongst the SMT of the forthcoming changes to the legislation in relation to data protection, to explore the likely impact and the immediate organisation wide actions required. The General Data Protection Regulations (GDPR) will come into force from 25 May 2018.

## 2. Strategic Context

The impact of the GDPR is dependent upon the nature of an organisation's business, the personal data it processes and what it actually does with that data. The clear and sensible advice is that organisations should carry out a data audit and mapping exercise. This would ensure that we understand clearly what are doing with both the data of students and employees across the organisation. Whilst these are the key groups impacted there will be others e.g. prospective/former employees and students, contractors, agency staff. This exercise would enable us to prioritise areas for action and identify what aspects of the GDPR will have the greatest impact on the College.

This audit would present some very useful intelligence about the data journey for students and staff as they travel through the organisation. This would be of benefit to the broader strategic project to integrate systems across the College.

The GDPR joins anti-bribery laws in having some of the very highest sanctions for non-compliance including revenue based fines of up to 20,000,000 Euros or 4% of annual global turnover. These fines could apply to breach of a data subject's rights or international transfer restrictions, for example.

The GDPR also makes it easier for individuals to bring private claims against organisations.

Where we fail to comply there are clear reputational risks for the College both with external stakeholders and with our staff and students.

However, I think that the key to this is that if we as an organisation take the time to properly prepare for and comply with the new Regulations then we will not only avoid the risk of significant fines and reputational damage, but take advantage of the opportunity to improve our data handling and information security systems and our compliance processes and to ensure that our contractual, staff and student relationships are even more professional, robust and reliable.

### 2.1 The Brexit Question

UK organisations handling personal data still need to comply with the GDPR, regardless of Brexit. The government has confirmed that GDPR will apply in the UK, a position endorsed by the UK's Information Commissioner (ICO).

## 3. Summary

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA). On my analysis it appears that we are broadly compliant with the current law and so that means that most of our approach to compliance will remain valid under the GDPR and can be the starting point to build from. However, there are new elements and significant enhancements, so we will have to do some things for the first time and some things differently.

The first key task for the group will be to ensure that a desk top data audit and mapping process is progressed as a priority across core College personal data processes.

## 4. Discussion

There are a number of legislative changes but for the purposes of this paper and in the interests of relative brevity I simply highlight some those changes with the biggest implications alongside suggested actions:

### 4.1 Data Breaches

One of the most profound changes to be introduced for organisations is mandatory reporting of any data breach to the ICO within 72 hours of becoming aware of it. The notification must include specific information, including a description of the measures being taken to address the breach and mitigate its possible side effects. Where the breach may result in a high risk to the rights and freedoms of data subjects, the data subjects themselves must be contacted “without undue delay”. Notification of breaches will become the norm given the frequency that events which may constitute breach will occur such as lost or stolen devices or emails sent to incorrect addresses.

Failure to notify could result in a fine along with a fine for the data loss.
There is a legislative exception where the personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons – we will need to see how narrowly this exception is interpreted in practice.

**Implications**
We should assess the types of data we hold and assess and document where notification would be required.

## 4.2 Requirement to Maintain Records of Personal Data Held and Processed

Organisations should document what personal data they hold, where it came from and who they share it with.

**Implications**

The carrying out of an information audit as a key action arising from this report would provide us with this baseline information and demonstrate compliance with GDPR.

## 4.3 Privacy Notices

The term ‘privacy notice’ is used but in fact this information can be provided through a variety of media – orally on the phone, website, email etc.

We need to ensure that where we gather personal data from individuals that they understand who we are and what we intend to do with their information. There are scenarios where it is reasonable for someone to expect that you will use their personal data for an intended purpose and you are not required to actively explain this to them but instead have information available and accessible if they look for it e.g. on our website.

Privacy notices, in printed form and actively provided, are required where there will be significant processing, which is not always reasonably foreseeable by individuals, such as for our students and employees. We currently advise our students in the student agreement of what we intend to do with their personal data. There will be other interactions where we seek personal data and either notify or should notify students clearly of what we are doing with their personal data and why we are doing it. The GDPR means that we need to ensure that this is consistently and clearly in place across the College. The scenario in relation to

our employees is similar, with the initial privacy notice being the contract of employment.

**Implications**

We should review our current privacy notices and practices and put a plan in place for making any necessary changes in time for GDPR implementation. I have already discussed this with colleagues and agreed that we will make the necessary changes in the student agreement in advance of the January enrolments. Our contracts of employment are to be reviewed by our external employment lawyers and I have agreed with the Director of HR that this is an opportune time to ensure that we have a clear and robust data protection clause.

Although we can endeavour to cover as many bases as possible in the student agreement (or contract of employment) it is probably not wise to rely on that as a cover all and provide additional privacy notices for other specific scenarios e.g. a student funding form, PLSP or, for employees, a referral to occupational health. This will ensure that we are giving individuals greater choice and control of their personal data.

### 4.4 Subject Access Requests

We will no longer be entitled to charge for requests and we have a month to comply instead of 40 working days.

**Implications**

Process changes required.

### 4.5 Lawful Processing

There will be a higher bar for lawful processing under the GDPR. This means that it will be harder to justify processing and sharing of data. The ability to rely on consent as justification for processing is made much more stringent, especially where there is a relationship where the processor is in a position of power such as the college in its relationship with students and staff.

**Implications**

The College will generally be processing data on the basis that it is **in fulfilment of a contract with the data subject** i.e. the student contract or employment contract. This condition does not justify sharing information where the contract is commercial in nature i.e. between the College and a third party.

We will need to review our standard contractual documentation and information sharing arrangements to ensure compliance with the GDPR. APUC has sensibly recommended that work starts now to review existing supply bases to establish where personal data is shared so that Colleges can understand what suppliers are 'GDPR relevant' and which are not and then to identify where existing contractual protection is insufficient for compliance with GDPR. This is another aspect of the data journey which we will need to consider.

### 4.6 Data Protection Officers

The College must have a Data Protection Officer (DPO), whose responsibilities are detailed in the GDPR as including responsibility for monitoring compliance with the Regulations, providing information and advice, and liaising with the supervisory authority. The legislation specifies that the DPO must be independent. This does not mean that organisations have to appoint an external person; the DPO role can be fulfilled by an employee. The post can be a part-time role or combined with other duties, but, in performing the role, the DPO must have an independent

reporting line. ICO guidance states that ‘it is important that the appointed person is a professional with “expert knowledge of data protection law and practices”.

**Implications**

The College should ensure that it has such a person in place. HR is aware.

## 5. Finance & Resource Implications

There are wide implications across the College. There will be some budgetary implications, not least for awareness training amongst staff, staff time in work related to this project, possible changes to IT systems, contracts and development of new processes. The implications will depend upon the gaps and improvements required as a consequence of the internal data mapping exercise and should be more easily quantifiable as a consequence of that process.