Colleges and the General Data Protection Regulations (GDPR)

The law on data protection in the UK will be significantly strengthened next year. Colleges, like all companies and organisations, need to anticipate this change and prepare now. The change in the law takes place at a time when individuals are much more aware of the value of their own data and the way in which it is used. Law or no law; this is an issue which colleges should focus on.

Some of the key issues for colleges to be aware of are:

- The new rules (GDPR) will take effect on 25 May 2018 via a Data Protection Bill which will be debated in Parliament in autumn 2017.
- Data collection should be minimised to what is necessary and there must be informed consent from individuals.
- Privacy notices must be clear about what the organisation will do with the data.
- Clear communication when obtaining data, particularly students is critical. A proportionate approach is also needed with former students.
- Review internal data systems to ensure information is kept securely and look into cybersecurity as data breach penalties are severely increasing.
- Review and adapt the way sensitive data (for example ethnic origin, disabilities, health status or criminal records) is managed and stored.
- Appoint a named Data Protection Officer, who has statutory tasks including advising the organisation and monitoring compliance.

These are explained in this paper.

Introduction

1. The General Data Protection Regulation (GDPR) is a European Union (EU) directive which takes effect on 25 May 2018, before the end of the 2017-18 academic year. The UK Government has confirmed that the directive will be put into law regardless of Brexit. On 7 August 2017, the Department of Culture Media and Sport (DCMS) published a statement of intent which confirmed that GDPR will be implemented via a Data Protection Bill which will be presented to Parliament in September 2017\(^1\).

\(^1\) Department of Culture Media and Sport, New Data Protection Bill, Our Planned Reforms 7 August 2017 https://www.gov.uk/government/consultations/general-data-protection-regulation-call-for-views
2. This note explains the implications of GDPR in a number of areas for colleges and highlights areas where they should already be taking action.

3. In the past government agencies might have provided detailed guidance and implementation plans on an issue like this. Now responsibility rests with colleges but AoC has a role in signposting important issues both to college leaders and to government officials.

The GDPR and colleges

4. The GDPR is described by the UK Information Commissioner as the “biggest change in data protection law for a generation” but it builds on existing data protection arrangements and – according to official ICO advice – should not cause significant problems for organisations that already take the issue seriously. The new data protection regime brings many changes which can be summarised as follows:
   - There will be different data principles set out on a stronger way.
   - There is an emphasis on accountability, including at Board level.
   - Individuals obtain new rights over the way their data is used.
   - Organisations need to issue longer privacy notices.
   - There will be a new system of breach reporting and higher penalties levied by ICO.

5. Colleges are long-established organisations with plenty of experience in handling data. AoC's initial assessment is that GDPR poses the biggest challenges in the following areas:
   - Making legally compliant changes to data collection on students which is a major exercise focused in August and September because of the annual turnover of students.
   - Ensuring that relatively old (legacy) IT systems provide sufficient protection for personal data.
   - Providing greater protection for sensitive data at a time of higher expectations that colleges will use such data to prevent extremism, safeguard students, overcome disadvantage and improve performance.
   - Developing adequate arrangements for communicating privacy notices to students and other data subjects.
   - Determining who the Data Protection Officer is and ensuring effective reporting lines to the governing body in circumstances where many colleges have slimmed down management teams.
   - Reconciling the new data protection law with their obligations under the Freedom of Information Act.

---

2 The Information Commissioner’s Office (ICO) is the UK agency with responsibility for ensuring data privacy for individuals alongside its work in promoting openness by public bodies.
Implementation of the GDPR

6. The GDPR was approved as EU law in 2016 and has 99 articles and runs to 88 pages\(^3\) In the June 2017 Queen’s Speech, the Government promised a Data Protection Bill which will implement GDPR. The DCMS statement on the bill published in August 2017\(^4\) sets out the government’s specific plans. The bill will also require major social media platforms to delete information about individuals at the age of 18, allow the police to continue to exchange information with international partners to combat terrorism and to update the powers available to the Information Commissioner’s Office (ICO).

7. Although the GDPR is fixed as a piece of EU law, work is continuing at an EU level on some of the guidelines that interpret it. A working party of European Data Protection Authorities set up under Article 29 of the regulations (and including the UK ICO) is formulating guidelines on consent and on other areas. There is a timetable for fixing some rules but we are still in a period where there is some fluidity on key points.

8. DCMS will not publish the Data Protection Bill until September 2017 and this will not become law before spring 2018 so the precise shape of the protection regime in the UK is not settled but colleges should nevertheless prepare now in certain key areas. The rest of this note identifies six key areas where preparation is needed.

Data collection on students

9. The new data protection regime strengthens the rights that individuals have over the data that organisations collect and process. This happens by creating or strengthening the obligations that organisations have with regard to personal data. These include:

- Minimising data collection to what is necessary.
- Consent arrangements. Individual consent to the use of their data must be “freely given, specific, informed and unambiguous”.
- More transparency about what organisations do with data. The term “privacy notice” describes the information given to individuals (or accessible to them) when data is collected.
- Stronger protection of data.
- Deletion of data when it is no longer needed or when requested.

---


10. Colleges need to address these issues for all the data they collect and process whether this is for students, staff, governors, suppliers, employers, parents or visitors whose image is captured on CCTV. The area which requires greatest attention is student data. Colleges collect considerable amounts of personal data from thousands of students each year often in a concentrated period of time. They hold this data while students are enrolled but also for many years afterward. They share the data with a wide range of public organisations who process it themselves and match the data received with other records. There are a number of steps that colleges should take with regard to their student data:

- Ensuring they have incorporated ESFA’s latest Individual Learner Record privacy notice they collect in their enrolment process. The latest notice was issued on 28 April 2017 as Annex F to the ILR manual and has not yet been updated to take account of the GDPR\(^5\)
- Making arrangements to communicate any update to the privacy notice to existing students whose data is already on systems when the new Data Protection rules take effect. The update may be necessary because of decisions or guidance by the college, the Education and Skills Funding Agency (ESFA), Department for Education (DfE) or ICO.
- Choosing a proportionate approach to communicating the college’s updated data protection arrangements to former students. Colleges have legal obligations set out in funding agreements, funding and audit guidance in relation to data retention. ESFA’s use of adult education funding to match fund European Social Fund (ESF) spending means that records have to be kept long into the 2020s\(^6\). The college should consider using its GDPR implementation to explain its retention policy in a clear and accessible way to students.
- Carrying out an internal review or audit of the way in which student data is kept, transferred, archived and deleted across the college by staff outside the main student record system.

11. Student data is the biggest area in colleges affected by the new data protection arrangements so should be tackled first. The same approaches and methods could then be applied and adapted to other data held and processed within the college.

Control of IT systems

12. The new laws require colleges to act on data protection but data breaches associated with cybersecurity failures are a more immediate reason for action.

\(^5\) Annex F of the 2017-18 ILR manual

\(^6\) ILRs and student record for the years from 2006-7 to 2014-15 have to be retained until March 2022 while those from 2015-16 onwards have to be retained until March 2030.
There have been a number of incidents where systems have been hacked, data stolen and, in some cases, published. JISC offers specialist advice on cybersecurity. GDPR raises the maximum penalty for serious data breaches from the current £500,000 to as much as £18 million\(^7\).

13. Colleges are expected to take technical and organisational measures to provide stronger protection for personal data. Their responsibilities extend to organisations processing data on their behalf. Techniques that could be adopted include minimising the data collected, anonymising before processing and creating ways to allow individuals to see their data. The expectation in the new rules (and an implicit expectation in the current regime) is that organisations will implement data protection by design and will carry out impact assessments before new uses.

Sensitive data

14. There are stringent expectations about sensitive data which apply to colleges because they collect data about self-declared ethnic origin and disability and also have information about the health status and criminal records of some students. GDPR prohibits the processing of data defined in the rules as being sensitive unless there is explicit consent for its use.

15. The new rules should not necessarily require changes to the ways in which colleges handle sensitive personal data but there are areas which might usefully deserve a review:
   - Colleges exchange a considerable amount of sensitive personal data with councils as part of the education health and care plan process. Is consent properly secured? Are the methods used to protect this data sufficient? Are there policies and processes to delete records when they are no longer needed?
   - Is sensitive data, which could be used maliciously to identify and possibly target a group of students (for example by ethnic origin), routinely available to large numbers of staff users or available only on a controlled basis?

16. The GDPR also introduces a new restriction on obtaining consent for the processing of children's data for “information society services” (this is an EU regulation). ICO summarises this as meaning that organisations must get parental consent for processing of data relating to children in all circumstances unless this is necessary to fulfil a legal obligation. DCMS plan to apply this threshold at age 13 which means that there is probably not going to be implications for online enrolment of students in Year 11 because the requirement would be on the college to obtain parental consent. Colleges should nevertheless consider what

\(^7\) The maximum fine will be 20 million euros. The biggest fine so far under current rules was a £400,000 fine paid by TalkTalk
arrangements they have for age-verification and whether they are taking reasonable steps to verify parental responsibility for those under the relevant age.

Privacy notices

17. GDPR extends the amount of information that organisations should give to anyone whose personal information is being collected, stored, processed and transferred. For colleges this means students, staff, suppliers, employers etc. It will make sense to make a general message accessible on the college’s website which covers all categories of data and then to supplement this for specific categories of data. GDPR compliance means extending privacy notices. They should include the following information:
   - Information about the college including contact details for the Data Protection Officer
   - The categories of organisations and people who will have access to the data (for example ESFA when it comes to student data)
   - What the data will be used for
   - How long the data will be stored
   - The legal basis for using the data - in the case of colleges relates to their power in the 1992 to provide further education.

Accountability to the Board via the Data Protection Officer

18. Colleges should take particular care on the governance and accountability aspects of GDPR because these will be immediately visible on implementation. The regulations require public authorities and organisations engaged in systematic processing of data to appoint a Data Protection Officer (DPO). AoC understands that the fact that colleges are covered by the Freedom of Information (FoI) Act means they will be considered public authorities for these regulations. We will check and, if necessary, challenge this.

19. The Data Protection Officer has a number of statutory tasks including advice to the organisation, monitoring of compliance and acting as the first point of contact for regulators (ie the ICO) and for individuals whose data is processed (ie students). The regulations say that they should report to the highest management level of the organisation (ie the Board), should have independence and should have adequate resources for their role. Colleges will need to think carefully about who is named as the DPO because the individual concerned should not have internal conflicts of interest. Depending on the college’s management structure and their responsibilities, possible candidates for the DPO role might be the Clerk/Company Secretary, HR Director or VP Quality. This role should not be allocated lightly and another solution might be to contract it out but this does not alleviate the college or the board of responsibility. ICO’s advice on governance is measures need to be “comprehensive and proportionate”. As a college sector, we will need to explore what this means on the basis of experience.
Reconciling data protection and FOI obligations

20. Compared to government departments, councils and more high profile public service organisations, colleges receive relatively few FoI requests but these can be burdensome in staff time and sometimes place colleges at a disadvantage compared to private training providers who are able to bid for contracts on the same terms as colleges without the same transparency obligations. English colleges are in a similar legal position to universities in that they are self-governing private sector charitable organisations for many purposes in public life but are covered by public service obligations when it comes to the FOI and similar laws. The reason why FOI is an issue to highlight is the fact that requests to colleges sometimes cause difficulty when they focus on information about specific individuals working at the college. Section 40 of the FOI Act provides an exemption from the duty to disclose information where it constitutes personal data, as defined by section 1(1) of the current Data Protection Act. The new data protection laws are not expected to modify the FOI rules in this regard but this is an area where care will need to be taken to balance conflicting obligations.

Further information

- Information and guidance on GDPR is available via the ICO website: www.ico.org.uk
- AoC will update this note regularly over the coming months. The next update is due 1 October 2017. Any comments, please contact Julian_gravatt@aoc.co.uk.
- AoC training workshops will be available in September and October:
  - The Impact of General Data Protection Regulation on Colleges Workshop (for administrators and marketing staff) - 29 September
  - The New General Data Protection Regulation Workshop (aimed at Data Protection Officers) - 19 October
- An HR-focused AoC webinar is available here https://www.aoc.co.uk/sites/default/files/GDPR-Webinar%20slides.pdf
- GDPR will be covered in our upcoming conferences:
  - AoC Clerks’ Conference – 16 October
  - AoC Employment Law Conference – 18 October

Association of Colleges
Updated 11 August 2017