Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Comment

UK further education sector journey to compliance with the general data protection regulation and the data protection act 2018

Benjamin Phillips[#]

Student with Solent University, Southampton UK

ARTICLE INFO

Keywords:
Data protection
GDPR
Further education
Data governance
Information management
Data subject rights
Data breach
Compliance
Public sector

ABSTRACT

The Further Education sector provides training and qualifications to 2.2million young people and adults annually and in the process collect a wealth of data which must be properly managed to ensure it is processed in a fair and transparent manner, maintaining compliance with good information governance and data protection legislation. This article shares the findings of a study which explored the content of General Data Protection Regulation action plans, first hand accounts from data practitioners and the views of students as provides embraced the new legislation.

The article demonstrates how a sector which fills the void between schools and universities is unique in the challenges they face when ensuring compliance with data protection laws. These challenges include the application of legislation, noting key differences between the nations of the United Kingdom, and the moral duties placed upon the provider by parents who expect open dialogue with the education provider, consistent as happened with lower levels of education. This must be balanced with the student's right to data privacy and control over who can access their educational records .

1. Introduction

May 2018 saw the implementation of the General Data Protection Regulation European Council (2016), also referred to as GDPR, introduced alongside the UK Data Protection Act 2018. Layton and Celant (2017) described the legislation as "the most monumental pan-European regulation in the last decade and may well become the world standard for data protection governance". The revision of data protection legislation has an impact on all businesses, globally, who collect and process personal data of those in the EU however, its application will differ between sectors and the types of businesses which make them up; affected by the organisation's purpose, structure, customer base and offering. This article is specifically interested with the impact upon the UK Further Education sector.

Further Education providers are data warehouses. As a result of their extensive reporting obligations to the government, funding bodies, data sharing activities with exam boards, safeguarding obligations and their own operational needs, vast quantities of personal and special category data are collected from 2.2million students every academic year

E-mail address: 3PHILB86@solent.ac.uk
[#] Home Address: Rose Cottage, Walderton, West Sussex, PO18 9EA

https://doi.org/10.1016/j.clsr.2021.105586
0267-3649/

Association of Colleges (2019). Statutory retention schedules mean collectively these providers are holding records on no less than 15million students at any one time. Combined with an underinvestment in critical information technology infrastructure and cyber security as a result of real world cuts in funding, this makes the education sector a prime target for cybercriminals (Charnock and Chapman 2020; Maguire 2019). Providers therefore have a duty to implement strong information governance procedures with appropriate safeguards to protect the vast quantity of data they hold from both human error and sophisticated cybercriminals.

To establish the current data protection landscape of the UK Further Education sector, during the 2019/20 academic year the researcher conducted a study which critically analysed the approaches to General Data Protection Regulation and Data Protection Act 2018 compliance within the UK Further Education sector with the aim of identifying best practice and common challenges. As a new piece of legislation affecting an under-resourced sector, the researcher explored the strategies and real world impact of internal action plans on information governance resource and the educational provider's ability to respond to data subject requests and manage personal data breaches. The research was conducted with the input of providers, students and data practitioners from across the Further Education sector to understand the practical implications of the new legislation. The findings were subsequently used by Further Education providers to benchmark themselves against the sector and to inform their own information governance practices.

2. Research methodology

The findings of this study were collected through empirical research. The best practice and common challenges outlined in Section 1.10 of this article have been formed through the study of a particular phenomenon at a particular time.

This was the first study of its kind which invited the entire sector to participate. Three data collection methods were used to capture qualitative and quantitative data. The first being a freedom of information request, distributed to 330 Further Education providers across all four nations of the United Kingdom with a response rate of 76%. The responses captured a baseline of quantitative data to deduce common practice and experiences. These findings were built upon through a series of semi-structured interviews with data practitioners working within the Further Education sector. Interview participants were chosen based on their role within their organisation and the knowledge they held. The final data collection method, a focus group of 40 current Further Education students provided the student perspective to this study. The student participants, who formed the student leadership team for a College Group, voluntarily provided their age, gender, subject of study and post code to ensure the focus group was representative of the diverse student population.

Multiple data collection methods and sources have contributed to the rich findings of the study, demonstrating the impact of GDPR in Further Education from both an institutional and student perspective.

3. Europe and the United Kingdom

In discussing European legislation it is important to establish the context of the legislation.

The European Union is an economic and political union, consisting of 28 member states European Union (2019a) across the 4 million km2 of land which is home to 513million inhabitants European Union (2019b). United through a set of shared goals and values, member states remain sovereign and independent states while delegating some decision-making powers to shared institutions to democratically decide on specific matters of common interest European Commission (2019). This includes the creation of European laws, standards and frameworks including those concerned with the use of personal data.

The United Kingdom is a sovereign country, consisting of the nations: England, Scotland, Wales and Northern Ireland; located off the northwestern coast of mainland Europe (Barr et al. 2019). The UK has a collective population of 66.4million inhabitants Office for National Statistics (2019) and at the time the study took place, was still going through the Brexit transition period.

4. Data protection laws

Data protection laws are concerned with the concept of privacy. The term privacy is highly subjective making the concept of privacy hard to define (Kennedy 2019; Moore 2008); differing by culture and age group. Privacy is the state of being alone and not watched or disturbed by other people Waite (2012). It is also described as the freedom from interference or intrusion International Association of Privacy Professionals (2019). Millennials, born between 1981 and 1996, and Generation Z, born between 1997 and 2012, have grown up in a world of online social media where information is readily available and therefore may have differing views on what is considered intrusive comparative to an older generation (Moran 2016; Dimmock 2019). The varying definitions of privacy generally agree that privacy is when individuals have control over their data and who can access it.

The term privacy and the control you hold over your privacy can be explored alongside self determination theory which explores how your motivation in terms of being autonomous and controlled is affected by your human motivation and personality in social contexts (Deci and Ryan 2012). The theory says people have three basic needs: autonomy, competence and relatedness. Relatedness provides a sense of belonging. Competence allows you to feel confident within your environment and to become a mastery of the things that matter to you. Autonomy is where you are wholeheartedly behind the thing you are doing because your behaviour is self endorsed. Empirical research shows autonomously-motivated students thrive in educational settings and benefit further when the provider supports their autonomy Reeve (2002). Privacy will mean something different to each individual and therefore it is important that providers are transparent in the use of data, adopting a privacy be design and default approach, to allow their stakeholders to make autonomous decisions

about how their data is used within an environment they feel confident in. Data protection legislation is designed to protect privacy through empowering individuals, referred to as data subjects, to maintain ownership over their personal data and giving them the control of who can access it. This supports the principles underpinning self determination theory.

Data protection legislation originated from the human right to privacy, first entering European law in 1981 when the Data Protection Convention European Council (1981) was adopted by the Council of Europe. Legislation was created recognising the need to protect citizen's privacy while maintaining free flow of data between member states Guarda and Zannone (2009). In 1995 the legislation was revised becoming a directive European Council (1995) which was the last major revision of the European data protection law until the introduction of GDPR which was implemented in May 2018.

There was a need for the GDPR. Rowley (2016) described the directive as a "patchwork quilt of legislation that largely met the minimums". There was a need for a single harmonised data protection framework which has become a wake-up call for every organisation in Europe who historically saw data protection as a nuisance, an unnecessary and an unwelcome layer of bureaucracy Rowley (2016). The GDPR took account of the advancements in technology, the internet and communication methods which have enabled individuals and businesses to share and access data instantly on a scale never previously seen ((ROSER et al., 2019)). This recognises that we live in a world where business is not constrained by geographical borders and neither is the data being processed by these businesses. This statement is equally true for the education sector. According to the Higher Education Statistical Agency (cited in UK Council for International Student Affairs 2019) there were 468,336 non-UK domicile students in UK Higher Education for the academic year 2017/18 of which 142,715 were from the European Union. Additionally 853,000 people studied or trained abroad as part of an Erasmus+ program in 2018 European Commission (2020) and these numbers do not include the students travelling to the UK to participate in short courses to improve their English or undertake a Further Education qualification.

5. The further education sector

The Further Education sector is a critical part of the UK education system, defined as "any study after secondary education that's not part of Higher Education" UK Government (2019). In 2014 it became law in England to study some form of Further Education until the age of 18 ((THE GOOD SCHOOLS GUIDE 2020)). Collectively the sector provides education and training to 2.2million young people and adults annually and employs 116,000 full time equivalent staff Association of Colleges (2019). The Further Education sector is made up of different types of provider but, the majority of 16–18 year olds are taught at Further Education colleges.

Colleges are not for profit organisations governed by the department for education Stokoe and Haynes (2012) and while students are at the centre of everything they do, continual cuts in funding equivalent to a 12% drop per student since the academic year 2010/11 Institute for Fiscal Studies (2019), places providers under increasing pressure to delivery high quality education on fewer resources. Constraints on funding also add to the pressures placed on back office departments, with a need for them to justify their budgets, especially where the role does not have a direct impact upon the quality of teaching and learning. As explored later in this article, these financial constraints have had a direct impact on the financial investment which has been made into good information governance activities.

The Further Education sector has been subject to constant change and in its current state is "fragmented, complex and difficult to understand" (Edge Foundation 2020, p. 2). Since the 1980s, the further education sector has been passed between six separate government departments, overseen by 48 different Secretaries of State for Education and seen the introduction of 28 major pieces of legislation concerning the sector and provision of vocational and skills training Norris and Adam (2017).

In 2015 the Department for Education began an area review process to understand and address the increasing challenges in post-16 education (UK Government 2017). The reviews assessed providers long term viability, encouraging collaboration and making merger recommendations with a view of increasing the providers long term financial stability through the sharing of back office services Collins (2016). One back office service that could be shared was data protection, while recognising the increased workload a larger provider may bring. The merger process presents the challenge of bringing together two organisations which may have different approaches to data protection compliance. Data Protection Officers are faced with the prospect of aligning historic processes, hidden datasets and sub-cultures across each campus while demonstrating to senior leadership teams why the approach one or both of the colleges has been following post-GDPR is no longer suitable.

Aligning institutional practice is not something which will happen overnight, especially where the way of doing things has become an integral part of the provider's culture. Some of these changes will happen naturally while others will need to be incorporated into a strategic action plan. Data Protection Officers should be designated recognising their professional qualities and knowledge of data protection law (European Council 2016). They should be in a position where they are accessible by all stakeholders and they themselves can access the organisational resource they need to fulfil their statutory tasks. Several data practitioners highlighted the provider's resource constraints as a barrier, especially where they work within a smaller provider. While the merger process generates additional work, in the short term it also enables these tasks to expand beyond those with dedicated data practitioner responsibilities. Merger creates a need and desire for departments to review policies, produces and whole ways of working which in tern will include information governance activities. While a Data Protection Officer may have input into these changes, data practitioners stated the department will often take ownership for the change, allowing them to concentrate on working with senior management teams to drive the merger and interact with staff across the colleges to address concerns and deliver training and awareness on more controversial matters.

5.1. *Parental involvement in further education*

The extensive educational offering, complex reporting structures and the age range of learners means Further Education exists within its own bubble of legalities and parental expectations. The classification of Further Education means they are not schools but, equally they are not universities UK Government (2019). Guidance published to help educational providers prepare for the new data protection regime is open to scrutiny as debate forms around guidance application. Further Education providers criticised a toolkit issued by the Department for Education as being aimed at schools with little application to a Further Education setting. This same toolkit was further criticised by schools with accusations that the Department for Education failed to prepare schools for the change in legislation ((WHITTAKER, 2019)). Interview participants stated guidance from the ICO in the form of codes of practice and online resources were recognised as being valuable resources but were criticised for being too slow to be released. This lack of guidance from official sources has therefore resulted in the sector working together, using online forums and collaborating with local providers to build networking groups to share and agree the practice which they will adopt.

Further Education providers found further difficulty applying existing guidance when factoring in age, given students aged 16 and 17 years, living in England and Wales, are considered competent data subjects in their own right (European Council 2016) but are still classed as a child, with someone else having parental responsibility for them (British Government 1989). The United Nations definition of a child is everyone below the age of eighteen years unless under the law applicable to the child, majority is attained earlier ((OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS 1989)). For the United Kingdom, this definition is adopted within the two principal acts relating to the protection of children's rights - the Children Act 1989 (British Government 1989) and the Children Act 2004 (British Government 2004). In England, Wales and Northern Ireland parental responsibility continues up to the age of 18 years and in Scotland until 16 years of age (General Medical Council 2018). Parental responsibility is defined in Section 3 of the Children Act 1989 (British Government 1989) as "all the rights, duties, powers, responsibilities and authority which, by law, a parent of a child has in relation to the child and his property".

Some argue parents should be involved with their son or daughters education because at 16 to 18 years of age, the majority of Further Education students are still classed as children (Goodall et al. 2011; Education Scotland 2019; Fischer et al. 2015). While this is accepted, to what extent a parent or guardian should be involved with education and the level of access they should therefore have to personal data regarding academic progress, is one area of contention. Another view accepts Further Education students as verging on adulthood and being capable data subjects. The Information Commissioner's Office ((INFORMATION COMMISSIONER'S OFFICE 2018)) advises someone with parental responsibility should act on behalf of a child where the child does not understand their rights however, if the child is competent, to let the child act for themselves.

The United Kindom has ratified the The Convention on the Rights of the Child. The convention is a theoretical framework which sets out a set of universal principles for children as they develop towards a normative status of adulthood Lansdown (2005). Article 5 of the convention presents the concept of evolving capacities, requiring parents, extended family and the state to provide appropriate direction and guidance in the exercise by the child of the rights recognised in the convention (United Nations 1989). The term appropriate is key, as each child develops differently and the closer the child gets to adulthood, the more capable they are likely to be in exercising their own rights. Competency will also be dependant on the decision to be made and the seriousness of that decision.

According to UNICEF Lansdown (2005), the difficulty in assessing competency comes from a lack of effective definitions of competency and availability of skilled professionals to conduct the assessment. We therefore look to existing tests and agreed understandings in defining competency.

Article 8 of the General Data Protection Regulation (European Council 2016) sets the legal capacity to consent to information society services at 16 years old, but in the UK has been lowered to 13 years old (British Government 2018). While education is not an information society service, the reasoning behind this competency can be considered as part of the decision making for data sharing in the education sector.

Much of the thinking around defining competency has been in terms of medical. The case of Gillick v West Norfolk and Wisbech Area Health Authority [(Gillick, 1985)] ruled in the House of Lords that doctors should be able to give contraceptive advice or treatment to girls under 16 years old. While not set out in statute, the Gillick competency test has since been more widely referenced in determining whether someone has the maturity to make and understand the implications of their own decisions in non-medical contexts (NSPCC 2019). This could include whether a student aged 13 years understands how they are instructing their personal data to be processed.

Castro ((CASTRO et al., 2015)) argue it is in the best interest of the student for parents or guardians to be involved in education. Boonk(BOONK et al., 2018)) found small to medium positive correlations when reviewing 75 studies examining the relation between parental involvement and academic achievement. They also highlighted while parental involvement does not diminish as children grow older, the nature changes, from providing assistance in learning to fostering conditions for academic success. The researcher argues the Further Education provider does not need to communicate personal data to parents for conditions to be fostered to enable academic success.

One of the roles of a Further Education provider is to help students take responsibility for shaping their future and to develop their independence. Consideration should be given to how students are supported and what can done to give that independence throughout their college life. Education providers are able to provide a variety of support both internally and through local organisations, tailored to the needs of each learner. This support can range from academic to pastoral to safeguarding and as such it can be argued parental involvement would not always be in the best interest of the student, respecting a student's desire to be independent, the

mental mindset of the learner and considering the range of support options available.

Noting this, the researcher was interested to explore how Further Education providers approach parental contact from a data protection perspective. Data protection legislation clearly states you must have a lawful basis to process data. The sharing of personal data between a Further Education provider and a parent or guardian is a form of processing. The researcher received a response from 222 Further Education providers across the four nations of the United Kingdom in response to a Freedom of Information request which asked their lawful basis for contact with parents of students under the age of 18 where the communication is not related to safeguarding or welfare concerns. As shown in the below bar chart, the lawful basis is not consistently agreed upon with Further Education providers relying upon legitimate interests, consent or public task.

The bar chart shows consent is most widely used, replied upon by 55% of respondents. A further 7% of the sector only communicate with parents where it is in the vital interests of the student to do so, suggesting that they do not routinely involve parents or guardians in the education of their students. A further 8% of providers have stated they use contract as their lawful basis, part of the agreement students sign with the provider in choosing to enrol with them. As official authorities, 14% of providers have chosen to rely upon public task, 10% legitimate interests and 6% rely upon legal obligation.

Under consent, students have the ability to freely give and remove permission to the provider for them to discuss their performance and progress at their place of study with their parents. Under legitimate interests the provider would claim it is in the interest of all parties for the provider to communicate with parents. Public task is similar to legitimate interests but can only be used where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller European Council (2016). As argued earlier in this section, it is debatable whether communication with parents is necessary to perform their official task of delivering an education. Under legitimate interests and public task, students have to use their right to object to stop this communication.

The researcher believes consent is the most appropriate lawful basis as it gives the data subject the greatest control over how their data is used and ability to enforce their rights. This view was shared by a student focus group who voiced the opinion that they, as students, should have the final say over who has access to their personal data. One student made the comparison that they would be unable to visit their parent's workplace and ask how their mother or father was performing at work and therefore the same should be the case for themselves as students. The students recognised in limited circumstances such as in an emergency or following a safeguarding incident there could be a need to share limited data with family members but, they felt strongly that where possible the student should be consulted first. The researcher believes that a provider should adopt a privacy first approach where it only demands and shares the information required to provide their service of education, everything else should be discretionary. This is a concept know as privacy by default and forms part of the General Data Protection Regulation.

6. Good information management

Governance refers to decisions and the people who make the decisions to ensure effective management and use of resource, whereas management is concerned with implementing decisions ((FU et al., 2011); Khatri & Brown, 2010 cited in (ALHASSAN et al., 2016)). An organisation with good information management will find it easier to comply with data protection legislation. Having the ability to demonstrate how systems and processes enable the organisation to understand the data they hold and how it flows throughout the organisation will improve both accountability and transparency. Unfortunately research by Price and Evans (2013) demonstrates despite organisations recognising the importance of information to their business operations they also acknowledge their information management practices are substandard. For many, if finance was managed in the same way as information assets, the organisation would be bankrupt within a week Price and Evans (2013). The researcher believes, following their research study, that the same would be true for many Further Education providers.

6.1. *Data mapping*

The need for good information management is not new, especially for the Further Education sector who have requirements to comply with Freedom of Information legislation and vast reporting obligations to the government, funding bodies and exam boards. It is said that every business activity is undermined by data, information and knowledge Price and Evans (2013) and this is particularly true in education where government and funding requirements require providers to collect significant amounts of personal identifiable information on every student and staff member, often held in a central digital database. The retention schedules attached to these records mean providers keep several years of data and despite greater adoption of electronic databases, there are vast quantities of historic paper records held in archive boxes onsite and in offsite storage.

Despite the volume of data held across different platforms, the concept of a data inventory, mapping the data and its flow across the whole organisation, is something providers have historically been unable to justify allocating the financial and human resource required to accurately complete. For this reason data mapping appeared consistently on GDPR compliance action plans.

For the first time, Further Education providers have had a legal obligation to establish what information they hold, why they hold it and document this. In interviews with Further Education staff with data protection responsibilities they described data mapping as a valuable exercise for the sector, giving them an opportunity to understand data flows and identify large, often unnecessary document stores which had been inherited as part of the area review merger process discussed in Section 1.4. They spoke about the benefits in reducing the amount of data they hold, clearing out

offsite archive stores and creating financial savings in document storage. Data practitioners also spoke about the often unforeseen benefit both data mapping and the wider GDPR compliance projects brought to their IT infrastructure. As a direct result of data protection projects redundant servers were decommissioned and an increased focus was placed on IT security, with some providers investing in migrating away from outdated infrastructure and improving cyber security to make the provider less susceptible to a cyber attack.

6.2. *Data protection officers*

In order to deliver change you require buy in from management teams and a person driving data governance activities. Good data governance must be embedded throughout the whole organisation. A Data Protection Officer is well placed for this role. Article 37 of the GDPR (European Council 2016) made the role of a Data Protection Officer mandatory where the organisation is a public authority, where processing activities are large scale or there is regular and systematic monitoring of data subjects. It can be argued the classification of a Further Education provider and the volume and velocity of data processed, requires a Data Protection Officer to be appointed. The appointment of a Data Protection Officer and the level of financial investment is one measure of how seriously Further Education providers take information governance responsibilities, especially giving consideration to the worsening financial position of the sector. Out of 245 Further Education providers, Freedom of Information responses show 17.5% outsourced their Data Protection Officer either to the private sector, or a shared services company. Shared service companies were seen predominately in Scotland and where providers are part of a parent company or trust. Participants interviewed as part of this study spoke of the benefits gained from economies of scale through the provision of shared data protection services provided in their ability to align best practice and establish robust information sharing agreements consistently with major stakeholders including funding bodies and local government departments. They also highlighted the ability to distribute capacity to the providers who need it most when large or complex data subject requests are made.

Where a Data Protection Officer remained in house, Freedom of Information responses have shown it to be common practice for the role to be amalgamated into the roles of: the Head of Information Technology, the Management Information Systems Manager, the Clerk to the Corporation or another senior manager such as the Principal or Assistant Principal. Article 38 of the regulation (European Council 2016) outlines independence as one of the requirements for the Data Protection Officer role. The Article 29 Working Party (2017(ARTICLE 29 WORKING PARTY 2017a)) list such roles within their guidance document as examples of where a conflict of interest would exist if the Data Protection Officer held such a position within the organisation. These roles will require the staff member to make decisions about how data is processed and it would therefore be argued full independence can not be achieved. A small handful of providers have used job sharing to mitigate situations where there is a conflict of interest but this could create further complications with demonstrating accountability.

Out of 245 providers who provided a response, only 21 providers internally appointed a Data Protection Officer where the scope of their job role is limited to information governance tasks, enabling them to have the full independence required by GDPR. 16 of the providers disclosed the pay scale for the role. The mean average minimum pay was £32,918 and the mean average maximum pay was £39,330. Comparable with online job marketplaces, this is above average for the education sector of £27,000 - £32,500 (Totaljobs Group Ltd 2019) but below the median for the role across the range of industries in the United Kingdom of £42,283 Neuvco (2019). A Further Education provider appointing a dedicated Data Protection Officer demonstrates, despite the financial constraints on the sector, they are committed to good information governance and achieving compliance with the legislation.

The strategic direction of data protection compliance sits with the Data Protection Officer. Only five providers had more than one person internally employed working solely on data protection compliance activities. However, many Officers are supported by staff in information technology and student records departments who have basic levels of data protection knowledge to support with helpdesk enquiries and responding to data subject right requests. These tasks are carried out alongside their main work outside of data protection.

7. Data subject rights

A strong data map and employees whose main role is to deal with data protection queries will help a provider in responding to data subject rights and in meeting their statutory timeframes. Data protection legislation provides data subjects with eight rights including the right of access and the right to erasure. GDPR has made the use of data subject rights more accessible, removing the £10 fee for accessing data and reducing the response timeframe from 40 calendar days to one calendar month. Data Protection Officers have made the observation, from their interactions with data subjects under both the 1998 act and GDPR, that data subject right requests are often made because people are angry or upset with something rather than just because the right exists. The role of the media in publicising the introduction of GDPR is recognised as a contributing factor to Data Protection Officers' perception that people are more aware of their rights. They note that people are quicker to reference data protection legislation in correspondents but do not fully understand how the letters G D P and R link with the request or statements that they are making. This can be partially attributed to the level of fake news which spread through social media, particularly around the lawful basis of consent in the approach to May 2018 (Strawbridge 2018; Hern 2018; Salsbury 2017; Field 2017), with many providers having to re-educate staff and students and myth bust current misconceptions of the legislation.

You could be forgiven for thinking that it would be fair to have made an assumption that Further Education providers would have received at least one right of access request in the first year of GDPR becoming enforceable. However, 64 providers who responded to a Freedom of Information request claim to have not received any right of access requests between 25 May 2018 and 25 May 2019. Research also shows

right of erasure requests are less common with 193 providers having not received a request in the first year from 25 May 2018. This could suggest an accurate record of data subject requests has not been maintained. Especially given the lack of providers appointing a dedicated Data Protection Officer to oversee such requests. It may also indicate there is a gap in staff training to be able to identify and escalate right of access requests to the staff member responsible for data protection compliance. More optimistically, it may suggest some organisations are better at being transparent in the way they use personal data with the systems in place to make frequently requested personal information readily available to the data subject.

Where data subject requests were received, on the whole, providers were able to respond effectively. 98.4% of providers who received right of access requests and 87.3% of providers who received right or erasure requests had fulfilled all the requests they received in the first year of GDPR within the statutory one month response timeframe. This is testament to the strength of information governance frameworks implemented within providers. In the event that response timeframes had to be extended, respondents highlighted complexities in the requests made rather than a failing in their processes as the reason for applying the extension.

Responding to data subject requests can be a resource intensive task for Further Education providers with vast quantities of personal data held across a variety of independent databases and manual filing systems. It highlights the need for a comprehensive data map and can contribute towards the justification to appoint a Data Protection Officer to relieve pressure on staff who are critical to the smooth running of day to day activities. Someone in a dedicated role with knowledge of the legislation will also help to accurately and consistently apply exemptions and redact documents.

8. Personal data breaches

The occurrence of a personal data breach is another critical part of data protection legislation which has to be managed by Further Education providers. Despite the safeguards and mitigations taken through comprehensive polices and technical safeguards, it is inevitable that someone will mishandle personal data at some point in time.

Cyber criminals also threaten personal data. According to Whitehead (2019) the UK education sector has a reputation for being easy targets for cyber criminals. One in five schools and colleges have been a victim of cyber crime, a figure compatible with the 26% of educational institutions who admit to not being fully prepared to deal with cyberattacks Ashton (2018). Your system is only as secure as its weakest link, who are often the people targeted through social engineering. The National Cyber Security Centre ((NATIONAL CYBER SECURITY CENTRE 2019)) reports “many cyber incidents at colleges are caused by untargeted attacks”. To test technical and operational safeguards JISC conducted penetration testing on 50 UK Universities and in 100% of cases were able to access high-value personal and research data within two hours Coughlan (2019) further demonstrating the scale of the issue.

The type of data held on students by schools and colleges may include mothers maiden name, national insurance number and bank details, making them targets for hackers and criminals who may wish to commit identify theft (Parent Coalition for Student Privacy and Badass Teachers Association 2018). The threat is real. In March 2019 a staff member at a UK secondary school opened an attachment containing a virus within a spoofed email, subsequently infected the school network with ransomware resulting in the loss of year 11 coursework (Welch 2019; Wakefield 2019). Innocent actions can cause significant problems and unfortunately are more common than the public may think.

8.1. *Internal data breach register*

EU data protection legislation puts an obligation on data controllers to internally record all personal data breaches which occur. The GDPR gives a wide definition of a personal data breach covering the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (European Council 2016). If applied to the nth degree, this definition would capture every malicious attack and accidental action of every member of staff or contractor who processes personal data on behalf of the provider.

Despite this only 179 Further Education providers, representing 72% of respondents, claim to have experienced at least one personal data breach in the first year of GDPR. 21 of these providers internally recorded a minimum of 20 breaches for the 12 month period of which 6 of the providers operated across five or more campuses and 18 had an internal Data Protection Officer. These providers do not come from any one geographic location, distributed across all nations and regions of the United Kingdom. The largest number of breaches recorded internally by any one provider was 81 personal data breaches but it should be noted that their size might be a contributing factor to the larger figure.

Of concern, 70 Further Education providers claim to have not experienced a personal data breach in the first year of GDPR. While not impossible, the broad definition of a personal data breach makes this unlikely. The researcher suggests poor record keeping or the providers interpretation of what fits within the definition of a personal data breach differing to staff at other providers, may influence this statistic. The data shows no correlation between a providers characteristics and the number of breaches they internally recorded, demonstrating no one type of provider is better at preventing or recognising personal data breaches.

8.2. *Reportable breaches*

There is an obligation to report personal data breaches to a supervisory authority where it is likely to cause a risk to the rights and freedoms of the data subject. The supervisory authority for the United Kingdom is the Information Commissioner’s Office. Freedom of Information responses show collectively the sector internally recorded 1529 personal data breaches between 25 May 2018 and 25 May 2019 of which 101 breaches met the threshold to be reported to a supervisory authority; equivalent to 6% of breaches experienced.

Of the 179 providers who experienced personal data breaches, 61 providers escalated breaches to a supervisory authority. In a Freedom of Information response made to the Information Commissioner's Office they confirmed they were processing 1915 items of casework for the education sector, which includes schools, colleges and universities, for the same time period. The Information Commissioner's Office was unable to filter this figure to only show Further Education providers, within the cost limits as laid out in the Freedom of Information Act, due to the limitations in their outgoing casework management system.

Accommodation must be made for the small percentage of providers in the Further Education sector who did not respond to the study and for the fact some breaches may have been reported to a supervisory authority in another member state. However, this data would suggest that Further Education was responsible for approximately 5% of reportable personal data breaches in the education sector and therefore comparatively, they have robust safeguards in place to protect personal data and mitigate personal data breaches. The researcher would argue that with further contextualised guidance to providers on what constitutes a personal data breach and improved record keeping, all providers will have experienced one or more personal data breach and the figure of reportable data breaches could be higher.

9. The student perspective

Students told the researcher that it is not until a personal data breach occurs that they have a reason to question the security of their personal data. Students are arguably the most important stakeholder of Further Education providers and are at the centre of everything the provider does. A student focus group has shown Further Education students have a good level of awareness for data protection and the impact it has on them. The focus group was representative of 16 to 18 and 19 plus learners and covered a variety of academic and vocational subjects. The focus group participants were able to identify a range of basic personal identifiers but were less appreciative of their digital footprint and how social media channels and online marketplaces use their data to build a profile of them. They did not appreciate how digital products could combine multiple datasets from across their platforms to gain a greater understanding of their customers and the ways they interact with their service. This immaturity was further seen as students openly admitted to exchanging their email address and other personal details in exchange for free WiFi access.

Despite the need to be educated on protecting their data online, students generally had a good appreciation for the value their personal data holds and the potential consequences which can occur through personal data breaches and by leaving social media privacy settings open. Students were also aware of the dangers of social engineering. During an interview with a Further Education Data Protection Officer, an incident was recounted of students refusing to give details to a marketing agency acting on behalf of the provider because the students were not expecting the phone call and the number used by the agency had a different area code to that of the educational provider. This is one example of many examples given by data practitioners where students refused to give out information to untrustworthy recipients or where they raised concerns that they considered their data to be subject to a personal data breach, for example when their personal email address gets disclosed in the 'to' field of a mass email being a frequent occurrence.

The same student focus group showed students trust their Further Education providers to look after their data. Students do not have a big brother view of their provider despite the large volume of data they process on a daily basis which can be attributed to the purpose of Further Education providers and the part they play in society. This trust is good because if the student wants to study with that particular provider, it is recognised they have no choice other than to share the data requested. But is this trust misplaced? What guarantees can a Further Education provider give to current and prospective students that the vast quantities of data, including special category data, are kept safe?

Transparency in data protection practices will build and maintain this trust. To be transparent a provider must have systems and processes in place to safeguard data, as has been discussed throughout this article. Privacy notices are a key document in explaining to data subjects how their data is processed but data collected during this study shows few providers are convinced students take the time to read the notice or check what they are signing up too. A hypothesis confirmed by the student focus group. If students do not understand what they are signing up for, when relying upon the lawful basis of consent, it could be argued that the consent was not informed and as such may be invalid.

However, despite the lack of reading, students were able to identify a range of agencies who would have access to their data such as the Department for Education and exam boards. Students understanding of why privacy notices are often text heavy is a view that they exist to meet a legal requirement. While true, it is the responsibility of educational providers, as data controllers to do more to ensure privacy information reaches all students. A data practitioner used the analogy of taking a horse to water. You can give the student a privacy notice but you can't make them read it. While understanding the logic to the statement the researcher believes Further Education providers have an obligation to make student friendly privacy notices. Article 12 of the GDPR requires privacy notices to be concise, transparent, intelligible and in an easily accessible form. Consideration should be given to the wide range of students who study with the provider, potentially making text heavy documents inappropriate for students with low levels of English or with learning needs. Some providers have experimented with visual privacy notices, using comic-strips and videos to engage learners in the way their data is collected, stored and used (Pembroke 2019; Wakefield College 2018; (CITY OF GLASGOW COLLEGE, 2018)). The use of layered privacy notices are recommended by the Article 29 Working Party ((ARTICLE 29 WORKING PARTY 2017b)) noting their ability to communicate a clear overview of processing activities. While there is no guarantee more students will engage with the privacy notice, it demonstrates a commitment from providers to improve transparency in their use of data and if done correctly will achieve its purpose. Similar initiatives have

previously been used by the supervisory authority and commercial businesses.

10. Learnings from the research

This study was the first to explore the strategies adopted to comply with GDPR enabling an analysis of baseline data on the level of compliance with the GDPR and the Data Protection Act in the United Kingdom Further Education sector, where the data is representative of the whole sector. The findings show a disjointed picture where practice has been built by the sharing of best practice through local networking groups and online forums. Data practitioners had criticised guidance intended to help comply with data protection laws for being too general and where designed for the education sector, as not inclusive of Further Education. Data Protection Officers working in Further Education are calling for definitive guidance to support them in their journey to data protection compliance and empowering students to take ownership over their data. It is the intention of the researcher that this study can act as the building blocks for data practitioners to develop their practice and raise the standard of data protection compliance across the whole sector. It does this by presenting the following common challenges and areas of best practice, identified through analysis of the study findings.

10.1. *Common challenges*

The challenges faced in achieving and maintaining compliance with the regulation by the Further Education sector exist both in the approach to and following the General Data Protection Regulation becoming enforceable. The following common challenges were identified through this study.

Continual budget cuts for the Further Education sector has resulted in some providers feeling unable to allocate the financial resource they would like to allocate to information management and governance initiatives. One interview participant identified the lack of finance as the direct cause for their provider not appointing a dedicated Data Protection Officer.

Only 21 Further Education providers in the UK have a dedicated in-house Data Protection Officer whose role is limited to information governance tasks. Evidence shows having a dedicated member of staff for data protection tasks ensures independence is maintained and can relieve pressure on business as usual functions when large data subject requests are received. Furthermore, they can act as a strategic lead in driving information governance throughout the whole organisation.

The size of the organisation is another reason, in addition to finance, some smaller providers believe they are unable to justify a dedicated Data Protection Officer role. Where the role has been consolidated into an existing role, the study has shown it is common place for a manager or a member of the senior leadership team to take on these responsibilities, creating a conflict of interest as they do not have the independence required by the legislation. It is a recommendation that providers who have resorted to this should allocate finance for an independent position as a matter of urgency to ensure they are compliant with this statutory obligation.

There is a lack of clear guidance designed for the Further Education sector to inform their data protection practice. Guidance published by the Department for Education has been criticised as being substandard, resulting in providers working together to identify what compliance means.

24% of providers did not respond to the Freedom of Information request made as part of this study and 50% of providers were unable to respond to the request within the statutory 20 working day timeframe. This highlights failings in providers abilities to respond to basic information requests.

The lawful basis for parental contact is not consistent across the sector. The jungle of legislation applicable to the sector and the complexities brought about by the age of Further Education students classing them as minors, and in England and Wales someone else having parental responsibilities for them, can be attributed to the confusion providers face in applying the lawful basis. 55% of providers have identified the lawful basis of consent as being most appropriate for this type of processing. It is the recommendation of the researcher that other providers consider changing to this lawful basis, adopting a data privacy by default approach and giving students the greatest control over how their data is shared.

1529 personal data breaches were internally recorded by Further Education providers, a figure which in reality is likely to be understated due to the 70 providers claiming to have never experienced a breach and the 24% of providers who did not respond to the request for information distributed as part of this study. This highlights a need to further educate staff on what constitutes a data breach and for additional safeguards to be implemented given 6% of data breaches experienced by Further Education providers met the criteria to be reportable to a supervisory authority.

10.2. *Best practice*

Despite the challenges faced, the sector has embraced the legislation. Providers have taken a risk-based approach to compliance recognising it is not a milestone and no large organisation can ever claim to be 100% compliant with the legislation. The study has shown the Further Education sector has made good progress against their compliance strategies having made good progress towards action plan tasks; with some providers using the new found focus on data management as an opportunity to drive efficiencies elsewhere in the organisation. The study highlights the following best practice.

Providers took different approaches to achieve compliance with new data protection laws based on their own understanding of the legislation and the impact it would have on their organisation. Through this independent approach, providers have consistently identified the same core tasks on their internal action plans to ensure a basic level of compliance with the General Data Protection Regulation. This has included the completion of article 30 documentation.

Staff at all levels of Further Education providers recognise the importance of the new data protection legislations and the impact it has on their work. It is evident, in the large majority of providers, that senior management teams and governors have bought into and support data protection compliance projects.

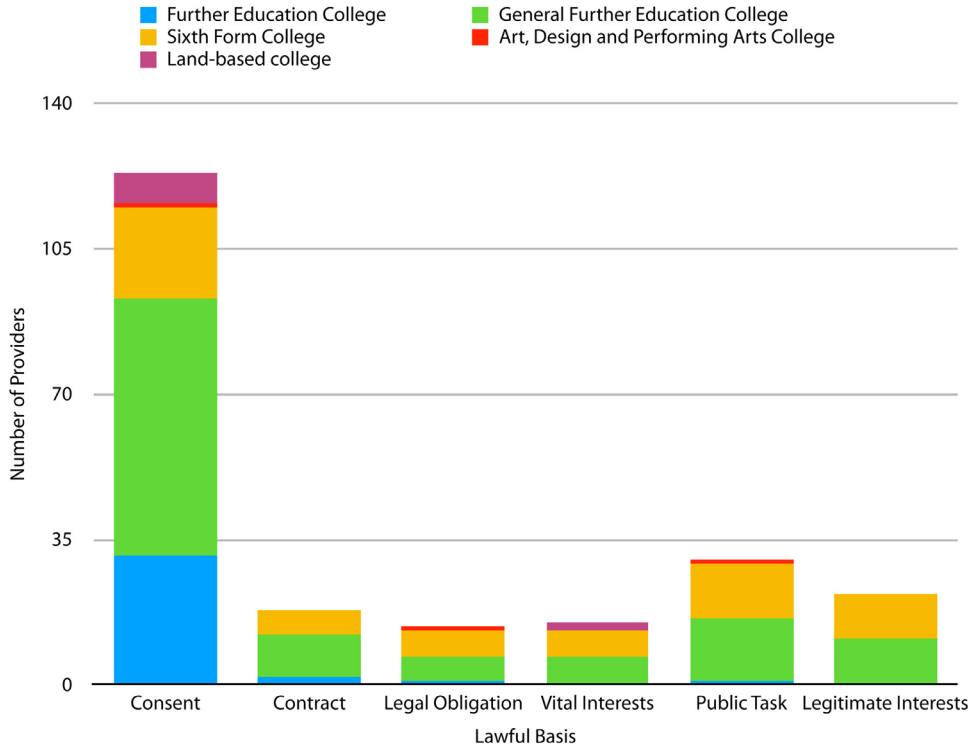

Fig. 1 – Lawful basis for parental contact by Further Education providers.

Students trust Further Education providers with their personal data. Providers should reinforce this trust through the provision of privacy notices designed to be understood and engaged with by Further Education students. Some providers have began exploring the use of graphical and video content as an alternative to text heavy documents. It is the recommendation of the researcher that other providers within the sector adopt similar strategies to engage students, particularly those classed as vulnerable and with lower levels of English, improving transparency in the providers use of personal data.

Staff are being up-skilled on GDPR and the impact it has on their day to day job and the major stakeholders of the provider. 98% of providers have released training to staff on data protection with multi-campus providers finding benefits in the use of e-modules to ensure a basic competency across the organisation reinforced through the use of face to face training sessions to enhance and personalise training for specific departments. Staff training is an effective means of myth-busting fake news but more can be done to help staff recognise what constitutes a personal data breach and how to escalate it to ensure internal breach registers and representative of the threats experienced by individual providers.

Providers have gained a greater understanding of the data in their care and how it flows around the organisation through the completion of data mapping exercises. As a result of data mapping exercises providers have undertaken data minimisation projects. Historic paper records and redundant electronic databases, outside retention schedules, have been identified and disposed of, reducing the amount of data and subsequent liability held by providers.

The General Data Protection Regulation has increased the focus on cyber security and projects intended to simplify IT infrastructure. Obsolete servers have been decommissioned and industry standard technologies embraced to improve the status of cyber security defences. The increased priority given to a more secure, simplified digital infrastructure estate gives the provider more control over their digital assets and reduces the likelihood of a cyber attack being successful in the future. Improved cyber defences will also enable providers to work towards the requirements of industry standards such as cyber essentials certification and ISO27001.

98.4% of right of access requests and 87.3% of right of erasure requests received by providers were responded to within the statutory timeframe of one calendar month, demonstrating the ability of staff to identify and escalate subject access requests and the effectiveness of internal processes in responding to the requests. Providers did highlight the impact on resource experienced when large or complex requests are received. Providers must ensure they can be flexible with resource to cope with any peak in demand and this may be further justification to appoint a dedicated Data Protection Officer.

11. Conclusion

Throughout this article, the complexities of good information governance and compliance with data protection legislation have been demonstrated in the context of Further Education. The data presented in this article has shown how a combination of a lack of sector specific guidance and the impact of real world funding cuts on institutional resources has contributed towards barriers in good information governance. However, the data also shows the resilience of the sector to work to-

gether to inform their own best practice and keep students at the heart of their core activities. The study has shown the benefits a data practitioner can yield in championing information governance strategies and action plans, especially in large providers or providers who have gone through a merger following the area review process. The good practice identified shows a positive trajectory for the sector as it continues to invest in building a culture of transparency in data processing activities that are supported by a privacy by default and design approach (Fig. 1).

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

The data that has been used is confidential.

Acknowledgments

Dr Esther Snell, who has provided guidance and critique throughout this study.

REFERENCES

ALHASSAN I, SAMMON D, DALY M. Data governance activities: an analysis of the literature. J. Decision Syst. 2016;25:64–75.
ARTICLE 29 WORKING PARTY, 2017. Guidelines on Data Protection Officers ('DPOs'). Brussels: European Commission [viewed 17 July 2019]. Available from: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
ASHTON, C., 2018. Cyber attacks hit a fifth of schools and colleges [viewed 5 January 2020]. Available from: https://www.itgovernance.co.uk/blog/cyber-attacks-hit-a-fifth-of-schools-and-colleges
ASSOCIATION OF COLLEGES, 2019. College Key Facts 2018-19. London: association of Colleges [viewed 4 January 2020]. Available from: https://www.aoc.co.uk/sites/default/files/College%20Key%20Facts%202018-19.pdf
BARR N, et al. United Kingdom. Encyclopaedia Britannica. Encyclopaedia Britannica, inc; 2019 Available from: https://www.britannica.com/place/United-Kingdom.
BOONK, L., et al., 2018. A review of the relationship between parental involvement indicators and academic achievement., pp.10–30 Available from: http://www.sciencedirect.com/science/article/pii/S1747938 × 18301027
BRITISH GOVERNMENT.. Children Act 1989; 1989 Available from: http://www.legislation.gov.uk/ukpga/1989/41/contents.
BRITISH GOVERNMENT. Children Act 2004; 2004 Available from: http://www.legislation.gov.uk/ukpga/2004/31/contents.
BRITISH GOVERNMENT.. Data Protection Act 2018; 2018 Available from: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.
CASTRO M, et al. Parental involvement on student academic achievement: a meta-analysis. Education. Res. Rev. 2015;14:33–46.
CHARNOCK L, CHAPMAN J. Cyber Security Posture Survey Results 2020: A snapshot of the Cyber Security Landscape in HE and FE. Bristol; 2020.
CITY OF GLASGOW COLLEGE. City of Glasgow College GDPR Intro; 2018 [viewed 15 September 2019]. Available from: https://www.cityofglasgowcollege.ac.uk/data.
COLLINS D. Area Reviews: FE Commissioner Letter; 2016 (October 2016) [viewed 22 March 2019]. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/560408/Further_Education_Commissioner_s_Letter_to_FE_Sector_Summer_2016.pdf.
COUGHLAN S. Hackers Beat University Cyber-Defences in Two Hours; 2019 [viewed 4 April 2019]. Available from: https://www.bbc.co.uk/news/education-47805451.
DECI EL, RYAN RM. Self-determination Theory. Thousand Oaks, CA: Sage Publications Ltd; 2012. p. 416–36.
DIMMOCK M. Defining generations: Where Millennials End and Generation Z begins; 2019 [viewed 28 April 2020]. Available from: https://www.pewresearch.org/fact-tank/2019/01/17/where-millennials-end-and-generation-z-begins/.
EDGE FOUNDATION 2020. Our Plan for Further Education: Defined, Career and Skills Focused, Collaborative. London.
EDUCATION SCOTLAND. Engaging parents and families A toolkit for practitioners Section 2: benefits of involving and engaging parents in their children's learning. Livingston: Education Scotland 2019 [viewed 26 March 2020]. Available from: https://education.gov.scot/improvement/Documents/par2-section2-mar19.pdf.
EUROPEAN COMMISSION. The European Union What it is and What It does. Luxembourg: Publications Office of the European Union; 2019 [viewed 1 December 2019]. Available from: https://op.europa.eu/en/publication-detail/-/publication/27bee15d-9ba9-11e9-9d01-01aa75ed71a1.
EUROPEAN COMMISSION. Erasmus+ Annual Report 2018. Luxembourg: Publications Office of the European Union; 2020 [viewed 4 June 2020]. Available from: https://op.europa.eu/en/publication-detail/-/publication/7985705e-41b7-11ea-9099-01aa75ed71a1/language-en.
EUROPEAN COUNCIL., 1981. No. 108 of 28 January 1981 on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Available from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
EUROPEAN COUNCIL., 1995. No. 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046
EUROPEAN COUNCIL., 2016. Council Regulation (EC) No. 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj
EUROPEAN UNION, 2019a. About the EU Countries [viewed 1 December 2019]. Available from: https://europa.eu/european-union/about-eu/countries_en#tab-0-1
EUROPEAN UNION, 2019b. EU in Figures [viewed 1 December 2019]. Available from: https://europa.eu/european-union/about-eu/figures/living_en
FIELD, T., 2017. GDPR: getting Past the 'Fake News' [viewed 22 February 2020]. Available from: https://www.bankinfosecurity.com/jonathan-armstrong-a-10084
FISCHER S, KILPATRICK S, BARNES R, SNOWBALL A. Equipping Parents to Support Their Children's aspiration: What works?. Launceston: University of Tasmania; 2015 [viewed 26 March

2020]. Available from: https://www.utas.edu.au/__data/assets/pdf_file/0020/920171/Parent-Project_Lit-Review_Final.pdf.
GENERAL MEDICAL COUNCIL, 2018. Definitions of children, young people and parents. Manchester: general Medical Council [viewed 5 January 2020]. Available from: https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/protecting-children-and-young-people/definitions-of-children-young-people-and-parents
Gillick v. West Norfolk and Wisbech Area Health Authority [1985]3 WLR 830
FU X, PALCZEWSKA A, NEAGU D, RIDLEY M, TRAVIS K. Data governance in predictive toxicology: A review. Journal of Cheminformatics 2011;3(24). doi:10.1186/1758-2946-3-24.
GOODALL J, VORHAUS J, CARPENTIERI J, BROOKS G, AKERMAN R, HARRIS A. Review of Best Practice in Parental Engagement. London: Department for Education; 2011 [viewed 26 March 2020]. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/182508/DFE-RR156.pdf.
GUARDA, P. and N. ZANNONE, 2009. Towards the development of privacy-aware systems., pp.337–50 Available from: http://www.sciencedirect.com/science/article/pii/S0950584908000578
HERN A. Most GDPR emails unnecessary and some illegal, say experts. The Guardian 2018 [viewed 22 February 2020]. Available from: https://www.theguardian.com/technology/2018/may/21/gdpr-emails-mostly-unnecessary-and-in-some-cases-illegal-say-experts.
INFORMATION COMMISSIONER'S OFFICE, 2018. Applications: children and the GDPR. Cheshire: ico.org.uk [viewed 19 July 2019]. Available from: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf
INSTITUTE FOR FISCAL STUDIES. 12% Fall Since 2010: Further Education has Faced the Biggest Cuts in Recent Years; 2019 [viewed 5 January 2020]. Available from: https://www.fenews.co.uk/fevoices/35320-further-education-funding-squeeze-set-to-continue.
INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS. What Does Privacy Mean?; 2019 [*viewed* 5 *January* 2020]. Available from: https://iapp.org/about/what-is-privacy/.
KENNEDY M. The Privacy Paradox/Dilemma in a UK Context: An Analysis of UK Data Subjects' Digital Privacy Attitudes and Behaviours post-GDPR. University College London; 2019.
LANSDOWN G. Innocenti Insight The Evolving Capcities of the Child. Florence; 2005.
LAYTON R, CELANT S. How GDPR Compares to Best Practices For privacy, Accountability and Trust. SSRN; 2017 Available from: https://ssrn.com/abstract=2944358 https://ssrn.com/abstract=2944358.
MAGUIRE D. Dealing With Cyber Security Threats to Universities and Colleges; 2019 [Online]. Available: https://www.jisc.ac.uk/blog/dealing-with-cyber-security-threats-to-universities-and-colleges-25-sep-2019 [Accessed 23 January 2021]..
MOORE A. Defining privacy. J Soc Philos 2008;39(3):411–28.
MORAN K. Social Media Natives: Growing Up With Social Networking; 2016 [viewed 5 January 2020]. Available from: https://www.nngroup.com/articles/social-media-natives/.
NATIONAL CYBER SECURITY CENTRE. It's Everyone's Role in Colleges to Embrace Cyber Security; 2019 [viewed 5 January 2020]. Available from: https://feweek.co.uk/2019/10/07/its-everyones-role-in-colleges-to-embrace-cyber-security/.
NEUVCO. Data Protection Officer Salary in UK; 2019 [viewed 3 April 2019]. Available from: https://neuvoo.co.uk/salary/?job=Data+Protection+Officer.
NORRIS E, ADAM R. All Change. Why Britain is So Prone to Policy reinvention, and What Can Be Done About it. London: Institute for Government; 2017.
NSPCC. Gillick Competency and Fraser guidelines; 2019 [viewed 19 October 2019]. Available from: https://learning.nspcc.org.uk/media/1541/Gillick-competency-factsheet.pdf.
OFFICE FOR NATIONAL STATISTICS, 2019. United Kingdom population mid-year estimate 2018 [viewed 4 January 2020]. Available from: https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/timeseries/ukpop/pop
OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS. Convention On the Rights of the Child. Geneva: United Nations; 1989 [viewed 19 July 2019]. Available from: https://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx.
BADASS TEACHERS ASSOCIATION. *Educator Toolkit for Teacher and Student Privacy*. studentprivacymatters.org: Parent Coalition For Student Privacy; 2018 [viewed 1 March 2020]. Available from: https://www.studentprivacymatters.org/wp-content/uploads/2018/10/PCSP_BATS-Educator-Toolkit.pdf.
PEMBROKE J. Privacy Statements; 2019 [viewed 24 January 2019]. Available from: https://www.jiscmail.ac.uk/cgi-bin/webadmin?A2=ind1901&L=FE-DATA-PROTECTION&O=D&P=5509.
PRICE J, EVANS N. Information asset management: who is responsible and accountable?. International Conference on Information Management and Evaluation. Reading: Academic Conferences International Limited; 2013. p. 129–36.
REEVE J. Self-determination theory applied to educational settings. Handbook Self-determination Res. 2002;2:183–204.
ROSER, M., E. ORTIZ-OSPINA and H. RITCHIE, 2019. Internet. Our World in Data. Available from: https://ourworldindata.org/internet
ROWLEY P. ITNOW; 2016. p. 48–9.
SALSBURY M. ICO Gets a Myth-Busting On GDPR; 2017 [viewed 22 February 2020]. Available from: https://socitm.net/blog/2017/08/17/ico-gets-a-myth-busting-on-gdpr/.
STOKOE P, HAYNES J. Abstract. Office for National Statistics.; 2012 Available from: https://webarchive.nationalarchives.gov.uk/20160107051314/http://www.ons.gov.uk/ons/dcp171766_266962.pdf.
STRAWBRIDGE G. The Top 5 GDPR Myths; 2018 [viewed 22 February 2020]. Available from: https://www.metacompliance.com/blog/the-top-5-gdpr-myths/.
THE GOOD SCHOOLS GUIDE. What is Further Education (FE)?; 2020 [viewed 26 March 2020]. Available from: https://www.goodschoolsguide.co.uk/careers/further-education/what-is-further- education.
TOTALJOBS GROUP LTD. What is the Average Salary For Data Protection jobs?; 2019 [viewed 3 April 2019]. Available from: https://www.totaljobs.com/salary-checker/average-data-protection-salary.
UK COUNCIL FOR INTERNATIONAL STUDENT AFFAIRS. International Student statistics: UK Higher Education; 2019 [viewed 4 June 2020]. Available from: https://www.ukcisa.org.uk/Research–Policy/Statistics/International-student-statistics-UK-higher-education.
UK GOVERNMENT. Further Education Courses and Funding; 2019 [viewed 20 July 2019]. Available from: https://www.gov.uk/further-education-courses.
UNITED NATIONS. Convention On the Rights of the Child. Geneva: United Nations Human Rights Office; 1989.
WAITE M. Paperback Oxford English Dictionary. 7th ed. Oxford: Oxford University Press; 2012.
WAKEFIELD J. GCSE Coursework Lost in Cyber Attack On Bridport school; 2019 [viewed 24 March 2019]. Available from: https://www.bbc.co.uk/news/uk-england-dorset-47551331.

WAKEFIELD COLLEGE. Wakefield College GDPR Spoof Video; 2018 [viewed 15 March 2020]. Available from: https://www.youtube.com/watch?v=s8SPF3yxAPA.

WELCH L. The Sir John Colfox School in Bridport was Targeted in a Cyber Attack; 2019 [viewed 5 August 2019]. Available from: https://www.dorsetecho.co.uk/news/17501187.the-sir-john-colfox-school-in-bridport-was-targeted-in-a-cyber-attack/.

WHITEHEAD E. Dangerous Data Breach At Swindon College Just the Tip of the Iceberg For the Education Sector; 2019 [viewed 5 January 2020]. Available from: https://evaporate.tech/dangerous-data-breach-at-swindon-college-just-the-tip-of-the-iceberg-for-the-education-sector/.

ARTICLE 29 WORKING PARTY. Guidelines On Transparency Under Regulation 2016/679. Brussels: European Commission; 2017b [viewed 25 April 2021].

WHITTAKER, F., 2019. *ICO receives hundreds of unnecessary school referrals as leaders struggle with GDPR* [viewed 15 March 2020]. Available from: https://schoolsweek.co.uk/ico-receives-hundreds-of-unnecessary-school-referrals-as-leaders-struggle-with-gdpr/