

Perspectives

Legal updates for the world of higher education



May 2019

Dear Colleague

On 8 May 2019 we held a special event at the Institution of Engineering and Technology in London to consider the implications of what some have called the 4th Industrial Revolution. This was attended by over 200 delegates from a variety of institutions engaged in teaching, research, business and the law. The phrase, the 4th Industrial Revolution, was first coined by Klaus Schwab, founder and executive chairman of the World Economic Forum in 2015. According to Schwab, this revolution is “characterised by a fusion of technologies” and “blurring the lines between the physical, digital and biological spheres”. We heard from our intellectual property partner Mark Pearce on artificial intelligence and James Fry our head of life sciences, both talking about the importance of these areas for the UK Industrial Strategy.

Creating new ideas in HE

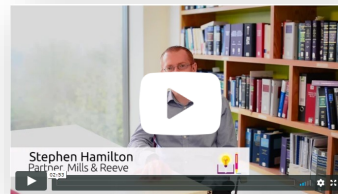
During the course of the day we heard from Professor Nick Petford, Vice Chancellor of the University of Northampton, about how they have been designing in technology to their new campus and from Adrian Ellison, Associate Pro-Vice Chancellor and Chief Information Officer at the University of West London, about how they have been investing in learner analytics to enhance the student experience.

We also heard from our construction partner Stuart Thompson and Rebecca Wade, Senior Bid Manager at Kier Construction, about how technology is being used in new ways in the design of project management for major construction projects.

Innovation

Principal Associate Poppy Short, one of our Innovation Champions, spoke about how we are embracing what new technologies might mean for us as lawyers and our clients and she highlighted some of the opportunities and issues arising in respect of ‘smart contracts’. Video material is available from the conference, including:

Cambridge partner Stephen Hamilton talking about the work we have been doing with [autonomous vehicles](#)

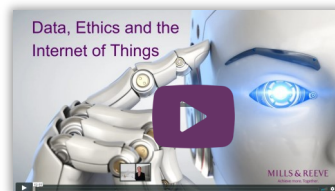


Manchester commercial partner Paul Knight talking about [block-chain](#)



Data, Ethics and the Internet of Things

Principal Associate Claire Williams highlighted some of the rules in this fast-moving area, including the concept in the GDPR of ‘privacy by design’. An article from Claire on cyber-security, first published in the June 2018 edition of Perspectives is included again in this edition for ease of reference. Claire also spoke about the ‘Internet of Things’ at the conference and some of what she said can be seen on her [recent video](#)



Included in this edition of Perspectives is an article from Principal Associate Emma Tuck on the Information Commissioner’s consultation on its code of practice on ‘age appropriate design’ for online services, along with articles from Christian Young on fraud recovery through private prosecutions and Christopher Bartley on new legislation affecting student tenancies and licences.

The world of work

Employment partner, Nicola Brown, challenged delegates at the conference to think about what the 4th Industrial Revolution might mean for the world of work and we asked delegates a number of questions to gauge their views. We asked delegates to vote on whether they thought that the 4th Industrial Revolution is a good thing, not a good thing or a question of design. This is what they voted:

- a good thing 32%
- not a good thing 6%
- it is a question of design 62%

We also asked delegates what was their greatest concern for the 4th Industrial Revolution. This is what they voted:

- its impact on work 3%
- its impact on privacy 24%
- its impact on equality 21%
- its impact on well-being 44%
- another concern 6%
- no concerns 3%

Of the other concerns identified by delegates, they highlighted: regulation vs ambition; data protection legislation and compliance; AI and replacing machines to do the job of people and the transition from legacy systems to new.

I spoke about the proposed new statutory duty of care contained in the Government’s recent White Paper on ‘online harms’ which was covered in the April edition of Perspectives. The Government’s consultation on the White Paper closes on 1 July 2019.

We have taken the challenge of the 4th Industrial Revolution to heart within Mills & Reeve too. Here is a [video with a spotlight on innovation](#) at Mills & Reeve.

Watch this space as the 4th Industrial Revolution continues to unfold...



Gary Attle
Partner
 +44 (0)1223 222394
 gary.attle@mills-reeve.com

In this issue...

“Age-appropriate” design for online services : ICO consults on draft code of practice

Page 3

Cyber Security: Top 10 cyber issues for universities

Page 4

Making Fraud Pay: Private Prosecutions

Page 5

Student tenancies and licences: significant legislation

Page 6



“Age-appropriate” design for online services: ICO consults on draft code of practice



Fresh on the heels of the publication by the Government of its [“Online Harms White Paper”](#) proposing a new regulatory framework for the digital economy to improve safety online, the Information Commissioner’s Office (“ICO”) has published a [draft code of practice](#) for online services likely to be accessed by children under 18, tying in with two of the ICO’s own published key strategic objectives: “to be proactive in identifying and mitigating new or emerging risks arising from technological and societal change” and the use of children’s data.


The draft code provides practical guidance on “...how to design data protection safeguards into online services to ensure they are appropriate for use by, and meet the development needs of, children”, focussing on the following 16 standards of age-appropriate design for information society services likely to be accessed by children:

1. The best interests of the child should be a primary consideration when you develop and design online services likely to be accessed by a child.
2. Age-appropriate application: consider the age ranges of your audience and the needs of children of different ages.
3. Transparency: privacy information must be clear and suited to the age of the child.
4. Detrimental use of data: do not use children’s personal data in ways that have been shown to be detrimental to their wellbeing / go against industry codes of practice etc.
5. Uphold your own published terms, policies and community standards.
6. Settings must be “high privacy “ by default.
7. Data minimisation: collect and retain the minimum amount of personal data necessary to deliver the elements of your service in which a child is actively and knowingly engaged.
8. Data sharing: do not disclose children’s data unless you can demonstrate a compelling reason to do so, taking into account the best interests of the child.
9. Switch geolocations off by default.
10. If you provide parental controls, give the child age appropriate information about this.
11. Switch options which use profiling off by default
12. Do not use “nudge techniques” (ie design features which lead or encourage users to follow a particular path, eg more prominent “accept” than “decline” buttons)) to lead or encourage children to provide unnecessary personal data, turn off privacy protections of extend their use.
13. If you provide connected toys (ie toys / devices that are connected to the internet), ensure you include effective tools to enable compliance with the Code.
14. Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.
15. Undertake a data protection impact assessment (“DPIA”) to assess and mitigate risks to children likely to access your service.
16. Governance and accountability: ensure you have policies and procedures in place to demonstrate how you comply with data protection obligations.

“Information society service” is defined in the Data Protection Act 2018 as being “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services”. In practice, most online services (eg apps, programs, many websites) will be ISS as remuneration needs not to come directly from the end user (so free services which involve advertising will still be ISS, as long as the services involve “economic activity” generally).

Importantly, the draft code works on the assumption that if you believe only adults are likely to use your service (ie the code does not apply) you still need to be able to demonstrate that is the case (eg market research etc). The scope of the code is therefore much wider than services marketed specifically for children.

The consultation on the draft code, which as and when finalised, will have statutory legal status (ie failure to comply may result in regulatory action and the code can be used in evidence in court proceedings) remains open until 31 May 2019, with the finalised code expected to come into effect before the end of the year after being laid before Parliament.

 [Emma Tuck, principal associate](#)
Emma.tuck@mills-reeve.com

Cyber Security:

Top 10 cyber issues for universities



Universities collate, process, and store a wealth of data. New research discoveries, commercially-valuable intellectual property, and the personal financial, health and other data of students, staff and others, are all contained within university servers. Implementing cyber defences and promoting an appropriate security-focused culture is vital for continued innovation, as well as crucial to protect your brand.

Five key operational considerations

Governance: Governing bodies, Vice Chancellors and other senior management functions are expected to drive the implementation of a cyber- and data protection culture, and be accountable in the event of a breach. Universities need to ensure they have implemented practical and enforceable security policies.

Marketing: In a competitive market, attracting the right students, investors and donors is essential. Changes in legislation mean that previous practices such as wholesale purchasing of contact lists without significant due diligence are no longer viable. Universities need to review and identify new, sustainable methods.

Data transfers: Cloud computing has numerous benefits, but in order to remain compliant with current data protection law it is vital that universities find out precisely where the servers they are uploading data to are located and what protections are in place. If they are overseas, you should have taken steps to ensure that the data remains secure and complies with GDPR requirements. Also, if data is processed on your behalf, does the contract specify the security measures required, and are you able to check they are in fact used?

Data processor contracts: Universities should continue to undertake appropriate due diligence checks on data processors before engaging them to process data on the University's behalf. They should also ensure that their contracts with data processors meet GDPR requirements, including obligations on the processor to take appropriate measures to ensure the security of its operations and systems.

Data management: Universities hold vast quantities of data, in both electronic and hard copy format, which they rarely access or use. Under the current law, personal data should not be held longer than is necessary to fulfil the purpose for which it was collected, and data minimisation is a central premise of the GDPR. At the same time, requests by data subjects for copies of the personal information that is held about them are on the rise. If you have not already done so, now is an ideal time to ask whether your organisation should continue to store these materials.

Five key cyber threats

Insider threats: It remains the case that most cyber security and privacy breaches are caused by malicious or accidental employee actions. Robust policies setting out protective measures, a sound understanding of data flows into and out of your organisation, and a well-designed and tested data incident response plan, will go a long way to preventing breaches or at least minimising their impact. Appropriate, interactive and targeted employee training is a necessary investment.

Bring your own device (BYOD)/mobile working: Students and staff use a vast array of laptops, tablets and mobile devices. The connection of so many personal items to your system brings with it the risk of malicious applications, targeted attacks which exploit known software vulnerabilities, and the theft of devices with open connections to a university's networks. You should have a clear, published approach setting out the measures that you expect to be taken to alleviate the dangers, such as software patching, password use and encryption.

The Internet of Things: Modern printers, photocopiers, televisions, thermostats, locks and even desk toys may be 'smart', transferring data to each other and their manufacturers. Software vulnerabilities and failure to change factory-set passwords can allow third parties to access and control devices, whether as part of a targeted attempt to access your servers, or in order to co-opt your devices for use in cyber attacks. Organisations should be alive to the dangers and take appropriate counter measures.

Outsider infiltration: Complex and data-heavy organisations like universities are a target for cyber criminals, who seek access via phishing scams, theft of user credentials or even physically accessing your premises to obtain papers or install malicious software. A robust understanding of potential entry routes will let you formulate appropriate policies and deploy defensive technological measures. The use of layered security measures and increased defences for particularly sensitive or valuable data will be expected by students, investors and regulators alike.

Impersonation and spoof emails: Hoax websites and spoofed emails, created to mislead readers pose dangers for universities. Cyber criminals use these tools to divert funds (such as by providing students with false account details into which fees should be paid), or to damage an organisation's reputation. Basic defences include purchasing domain names similar to your own and applying email validation systems such as DMARC.

 [Claire Williams, principal associate](#)

claire.williams@mills-reeve.com

Making Fraud Pay: Private Prosecutions



The PwC Report on Economic Crime 2018 indicated that 50% of UK Respondents to their survey had experienced economic crime in the past 24 months.

Of those who lost money 24% lost more than \$1m.

According to the NHS Counter Fraud Authority:

“fraud costs the NHS £1.29 billion a year - enough money to pay for over 40,000 staff nurses, or to purchase over 5,000 frontline ambulances. This is taxpayers' money that is taken away from patient care and falls into the hands of criminals.”

This is, of course, dastardly in the extreme but surely the long arm of the law will be bringing the criminals to book? Not quite.

A 2018 Which? report indicated that 96.3% of all cases passed on to Police by Action Fraud (the UK's national fraud reporting centre) went unsolved. If you find that difficult to believe then consider the written submission to the Home Affairs Select Committee by the City of London Police. It showed that in 2016-17, local police solved 3.1% of fraud cases, while 85% were unsolved, and 12.1% of cases were ongoing.

Not a clear up rate that Hercule Poirot would accept as reasonable. There are, of course, a whole host of reasons behind these figures and one might even dismiss them out of hand on the basis that there are “lies, damned lies and statistics”.

What can be done?

It would be reasonable to suggest that most people who are victims of fraud seek redress. Punishment by imprisonment or other penalty is not something that will replace the missing cash. If a criminal's assets are confiscated those items go to the state, not the victim.

This combined with low rates of detection has seen an increase in private investigation, prosecutions and civil recovery cases. In 2014 the Lord Chief Justice said:

“There is an increase in private prosecutions at a time of retrenchment of state activity in many areas where the state had previously provided sufficient funds to enable state bodies to conduct such prosecutions.”

Any individual or company has the right to bring its own prosecution in the criminal courts pursuant to S.6 (1) of the Prosecution of Offenders Act 1985.

Why bother? There are a number of advantages to bringing the case to court yourself.

- **Control** – you have the authority to dictate the way the case is shaped and progressed. Importantly you have the power to decide what may be acceptable to you in terms of pleas to charges that have been brought. You

can decide what if any compensation orders are to be sought. You will not have to rely upon an overstretched and under resourced CPS to make those decisions for you.

- **Costs** – unlike in civil proceedings, costs can be claimed from the Crown if you are successful. Even if you lose it is not a foregone conclusion that you will have to pay the defendant's costs, provided you can show that the case was brought with good cause and not in a malicious manner for an ulterior motive.
- **Speed** – criminal cases move through the judicial system at breakneck speed compared to the sometimes glacial pace of civil proceedings.
- **Publicity** – the impact of a successful criminal prosecution is so much greater than a successful civil case for no other reason than the morbid curiosity of the general public. Even if the case is lost the message that is sent out is that you, as an institution, will fight back.
- **Compensation** – this is a priority for you. It is not one that is necessarily shared by the Crown. The proceeds of a compensation order should go to the victim. The proceeds of a confiscation order will be paid to the state. Both can be sought in a private prosecution. In 2016 an Old Bailey Judge ordered that a defendant who had been convicted in a private prosecution pay a confiscation order in the sum of £20M to the State and a compensation sum of £18M to the victim.

A private prosecution is a powerful weapon in the armoury of a victim of fraud. The threat of civil proceedings makes less of an impact. It can facilitate a swift settlement of losses. Even if it does not drag the perpetrator to the table there are a number of tools organisations can use to investigate and uncover assets from which a settlement can be forced.

In many cases private investigators, forensic accountants and other experts (IT and software experts for example) can paint a telling picture of a fraudster's finances, often dispelling the lie that has been peddled that they are penniless.

In many cases it has been shown that the criminal who pleads poverty has properties abroad held by family members or holds other assets across the world.

Rather than discount the thought of action to recover a loss or accept a decision by the CPS not to proceed it may well be worthwhile considering action individually. As Lord Wilberforce said a private prosecution is “a valuable constitutional safeguard against inertia or partiality on the part of authority.”

 **Christian Young, principal associate**

christian.young@mills-reeve.com

Student tenancies and licences: significant legislation



There have been a number of recent legislative changes to the rules surrounding tenancies and licences in England. Considered below are the key changes in relation to student accommodation and exactly what this will mean for Universities.

Tenant Fees Act 2019

- This will apply to all new lettings from 1 June 2019 and will apply to existing lettings from 1 June 2020.
- It expressly applies to all student tenancies granted by Universities and to licences to occupy housing where the premises are occupied as a “dwelling”. The term “dwelling” does not have a fixed definition in law, leading to some uncertainty about whether it will apply to all types of student accommodation. Caution is recommended, however, in light of the penalties for non-compliance.
- The Act will prohibit landlords or their letting agents from requesting any payments from their tenants unless the payments are permitted under the Act.
- Rent is a permitted payment under the Act, however if the rent charged in a particular rental period is more than the amount charged in a later period, the additional amount will not be permitted, unless the rent being sought is proportionate to the length of the period. This will need to be kept in mind when charging varying amounts of rents to students for different semesters.
- Other permitted payments include: deposits (limited to certain amounts); payments in the event of default (only for losing keys/security devices or for failure to pay rent where the agreement specifically states the landlord can charge in these circumstances); payments on variation, assignment or novation of a tenancy (up to a maximum of £50 or, if higher, the actual reasonable costs to the landlord); payments on termination of a tenancy; and payments for council tax, utilities, television licences and communication services.
- Breaching the Act has serious consequences. A first breach can lead to a civil penalty of up to £5,000. A second breach is a criminal offence and can lead to an unlimited fine (or a civil penalty of up to £30,000 if the local authority decides not to prosecute the criminal offence).

- Mills & Reeve has produced a detailed guide to the Tenant Fees Act 2019 tailored for University clients and is happy to advise on whether a University’s precedent accommodation agreement contains any payments that will be prohibited under the Act.

Homes (Fitness for Habitation) Act 2018


- This will apply to all new leases (of less than 7 years) from 20 March 2019. The lease must be of a dwelling let wholly or mainly for human habitation. This does not include licences, and so will not cover certain types of student accommodation.
- The Act introduces an implied covenant by the landlord that the dwelling is fit for human habitation at the time of the grant of the lease (or at the beginning of the term) and will remain fit during the term.
- Landlords will have an implied covenant to be able to enter the dwelling at reasonable times of the day to inspect the condition of the property upon giving 24 hours’ written notice to the occupier.
- However the landlord will not be required to remedy unfitness when:
 - ◇ the problem is caused by the tenant’s behaviour or their possessions;
 - ◇ the problem is caused by events like fires, storms or floods, which are completely beyond the landlord’s control;
 - ◇ the landlord is unable to get required permissions, after making reasonable efforts; and
 - ◇ the tenant is not an individual, eg. Educational institutions.

If a landlord fails to comply with the Act, tenants can take court action, which may result in the landlord being ordered to pay compensation or carry out the works necessary to improve the property.

Deregulation Act 2015

- Please note, this Act only affects Assured Shorthold Tenancies (“ASTs”). This is only relevant to those Universities which provide tenancies of accommodation through a management company and the management company is the landlord.
- The Act applies in full to ASTs created on or after 1 October 2015 and in part to those created prior to that date.
- Various obligations are placed on landlords and failure to comply may impact the ability of the landlord to serve a valid section 21 notice. Key obligations placed on landlords include:
 - ◇ Landlords must supply tenants with a copy of the Department for Communities and Local Government ‘How to rent: The checklist for renting in England’ booklet at the start of their tenancy.
 - ◇ Before the grant of an AST the landlord must give the tenant a copy of the energy performance certificate and most recent gas safety report.
 - ◇ Deposits must be paid into a tenancy deposit scheme and landlord’s must comply with the initial requirements of the scheme and provide the prescribed information.

The Act includes other requirements and we would be happy to provide further guidance.

 [Christopher Bartley, principal associate](mailto:christopher.bartley@mills-reeve.com)
christopher.bartley@mills-reeve.com



About Mills & Reeve



Mills & Reeve offers a deep knowledge of the higher education sector and the commercial strength of one of the UK's leading national law firms.

Our multi-disciplinary team is ranked in tier 1 in the UK legal directories for advising the higher education sector.

We have supported our clients in over 75 jurisdictions through our international network of law firms around the world.

The Sunday Times has recognised us as a Top 100 Best Employer for the last 16 consecutive years; the only UK law firm to have achieved this. We work hard to create a culture where everyone feels that they contribute and can make a difference, delivering outstanding service to our clients.

