Chapter X

Online Safeguarding and Personal Cyber Skills for Students

Andy Phippen and Emma Bond

SUMMARY

The COVID-19 pandemic has driven universities to deliver education online, making use of digital platforms for both formal and informal learning. This move has accelerated concerns regarding institutions capabilities to protect students from online abuse and support those who fall victim to its many forms. Empirical data drawn from UK universities prior to the pandemic highlight the lack of policy and practice across the university sector around both awareness of, and support form, online abuse among the student body. Further concerns during the pandemic, which highlight failures not just of safeguarding policy, but cyber security practice, demonstrate the need for universities to not only recognize their duty of care regarding student welfare but also to provide training and education for all making use of online and hybrid higher education.

Keywords: Cybersecurity, Online harms, Online safeguarding

Prof Andy Phippen*
Bournemouth University, UK.
(e-mail:
aphippen1@bournemouth.ac.uk)

Prof Emma Bond
University of Suffolk, UK.

Corresponding Author

I. Introduction

This chapter considers online harms related to university students, with a particular focus on the move to online delivery caused by the COVID-19 pandemic. The transformation from face to face to online delivery was both novel and challenging for a lot of universities and we will consider the implications for this, particularly from the perspective of potentially placing students at risk as a result.

However, while the COVID-19 pandemic accelerated moves online delivery in institutions, more generally universities were moving over to online services for educational and social aspects of student life and this is also acknowledged in the chapter. In a book that considers the post-COVID higher education landscape, it is unquestionable that we will exist in a world where online delivery becomes not just an option, but desirable to a lot of students who perhaps have health vulnerabilities or they are international students who do not have the opportunity to travel to an institution to receive tuition face to face. We would also expect to see learning from institutions in how they delivered online education during COVID lockdowns to present new opportunities in terms of international teaching and asynchronous delivery.

With increased online delivery, and a post-COVID expectation of hybrid models of delivery that will undoubtedly grow, new risks for student welfare emerge and if institutions are providing online services in which students must engage for their learning, they need to acknowledge these risks and provide support for these. This chapter will explore what are often referred to as online harms, that result from these services and their use within the higher education content. It will consider what support students should expect from their institutions, and also explore a key legal issue around duty of care.
We will draw upon a case study and then evidence base taken prior to lockdown by way illustration of the state of a sector ill prepared to move to widescale online delivery and therefore why we are not surprised with the increased concerns around online harms are a result of online delivery, and how the COVID-19 pandemic has hopefully concentrated institutions on their duty of care around online harms.

The duty of care concept is an emerging legislative approach to addressing online harms (as will be discussed below) and presents some interesting challenges for those who provide online services. Universities, if they continue to move teaching and support services on to online platforms will undoubtedly have to reflect upon who the mitigate online harms in these settings, and their liability if they do not. However, the chapter also considers the need for responsibility on the part of the student themselves, and what knowledge they need to ensure they can mitigate risk online. In particular, an often-neglected

DOI: http://dx.doi.org/10.24018/ejedu.YEAR.VOL.ISSUE.ID

area of knowledge – the intersection between cybersecurity knowledge and online harms, will be considered, and we argue that being able to protect one's devices and digital assets is a key step is mitigating online risk.

II. The Online Safety Conundrum

The focus of this analysis resides in the UK Higher Education sector – this is the sector in which we both work and have conducted the data collection presented in this article. However, there is nothing UK specific about the behaviours we speak of and the attitudes of institutions.

Collectively, we come at this issue with around 30 years' experience researching and practicing in the area of online safeguarding. Therefore, there are some elements of this discussion that will have an ethnographic aspect to them – we provide advice for institutions on these matters as well as research them.

It has, from a personal view, been entirely predictable that institutions are now playing catch up around online safeguarding and the mitigation of risk in online environments. As academics working across a number of institutions in the UK we have always seen a reactive approach to online safeguarding issues (and sometimes, as discussed below, even opposition to the view that student welfare is the responsibility of the institution). We have researched a great deal in the statutory education sector in the UK (for example see Bond 2014 or Phippen 2016) and in this time we have seen a great deal of statutory pressure placed upon schools and colleges to ensure young people in their care are "safe" from the online harms that exist. We see little comparable pressure in the Higher Education Sector, yet. However, we have seen, as a result of high profile cases, as discussed later in this chapter, that regulators were beginning to raise concerns about student behaviours online, and how institutions respond to them, prior to the COVID-19 pandemic. All that the pandemic did was accelerate these concerns and focus thinking around the duty of care around institutions.

We have also seen, as a result of this work, the ideological challenge with ensuring safety when experiencing life online. There is an underlying challenge, which is writ large through online safety policy (again, see Phippen 2016) that we have to start from a position of prevention when considering "online safety and poses the question:

> *How can we make sure someone is safe online?*

A far more progressive approach would be, instead, to say:

> *How can we help people/our students be aware of the risks there are in being online, what are our responsibilities in making them aware, and what tools can we put in place to help them if they are subject to harm, such that we can reduce harm?*

This is, of course, a far more complex question to answer, but one that is at least achievable, in a way that the safety question is not. If we are to accept the definition of safe to be "Free from harm or risk of harm", this is an unachievable goal if we are to consider online harms.

III. Pre-COVID Concerns – The Warwick University Group Chat Scandal

In order to position this discussion and the challenges institutions face, we present initially a high-profile online abuse scandal that impacted upon a UK institution in 2019 – before the COVID pandemic. This case highlights the complexities of institutional responsibility prior to the pandemic, and reflects upon the fact that even before COVID-19, we saw a sector that did little to address the complexities of online harms. As we have stated above, the focus of most educational and policy discourses on online harms has remained for decades on school age children and teenagers centering around the media fueled topics such as cyberbullying and sexting. However, digital harassment and abuse continue to be experienced into adulthood but are not as well understood and certainly not as well recognized in academic and policy arenas. Poorly understood, digital harassment and abuse is defined by (Powell et al., 2018: pp. 199) as such:

> *Digital harassment and abuse refers to a range of harmful, interpersonal behaviours experienced via the internet, as well as via mobile phone and other electronic communication devices. Whereas much existing research has focused on the experiences of children and young people (including foremost 'cyberbullying'), there have been few international studies on adult experiences of digital harassment and abuse. As such, little is currently known about the extent, nature and impacts of digital harassment and abuse on adult victims. In particular, there exists a significant gap in current research into sexual, sexuality and gender based digital harassment and abuse.*

Within the university setting it is also important to consider that some people are more likely to experience online harassment and abuse than others. For example, as a result of gender, sexuality, ethnicity and disability and become victims of online hate crimes. Women are more likely than men to report being harassed online (Hess 2014) and are more than twice as likely to experience severe forms of abuse such as stalking or sexual harassment (Reid 2016). Yet as the higher education sector has increasingly moved to online delivery, the research examining experiences of harassment and abuse online in the university sector is scant (Veletsianos et al., 2018) and more broadly there relatively little research to date on adult experiences of online harassment and abuse generally with greater attention given to online identity theft, scams and online fraud. Yet as is clear from the example below, there is growing concern regarding online abuse in higher education and the response of institutions. Young women aged 16 to 24 years are widely recognized as being at greatest risk of experiencing sexual assault, and most often at the hands of a known man, such as a boyfriend, friend, or acquaintance, rather than a stranger (Henry and Powell, 2016). The high-profile media coverage around a particular incident, an online group chat case at the UK's Warwick University early in 2019 illustrated this clearly and began to raise concern regarding the sector addressing emergent harms effectively. In this case male students had been communicating about female students in a sexually aggressive and violent manner.

The online group chat named "Fuck women disrespect them all" was first reported by the media in late 2018 (BBC 2018), and as a result of that media coverage, the national broadcaster, the BBC, also produced a documentary later in the year where female students spoke of their experiences further. The Facebook group involved a group of male humanities students at the University talking about girls on their course including their names. Quotes from the group chat reported in the press included:

> *"Sometimes it's fun to just go wild and rape 100 girls."*
> *"Rape the whole flat to teach them all [a] lesson."*
>
> *"Rape her in the street while everybody watches,"*
> *"it wouldn't even be unfair".*

According to the BBC (2019) after an internal investigation at Warwick, run by their Head of Communications, one student was expelled and given a lifetime campus ban, two were given 10-year bans and also expelled, and two more were excluded for a year. However, after a review two of the men had their 10-year bans reduced to 12 months. Those who had been named in the group chats found themselves in classrooms with those who had threatened serious sexual assault.

Following the independent report which said the university needed to improve its procedures for dealing with sexual violence and misconduct, the vice-chancellor of Warwick University made a public apology to the female students who were victims of the 'rape chat' group. However, a legal case brought by some of the victims, which centers on negligence on the part of the institution, remains ongoing at the time of writing.

However, whilst the issues that the guidance is intended to address were brought to public attention by the case at Warwick University, we argue that this was not an isolated case. The extent of harassment, assault and hate crime behaviours in UK universities suggests that urgent actions are required (Hennelly et al., 2019). In the UK over the past five years there has been much rhetoric centered on changing the culture in higher education around student safeguarding and yet reality has borne out how difficult this is in practice and we question given the case at Warwick and many others whether any progress has been made. We argue that it is time to take a step away from talking about the need for change and instead, argue that is important that this this culture is actively challenged by all stakeholders, and not normalized. What is also important is that universities themselves do continue to be bystanders in these situations and as we are aware of this abuse happening on our campuses and beyond, we need to actively improve the level of proactivity and increase a victim focus that is currently sadly lacking across the sector.

IV. The Unhelpful Digital Natives Narrative

Throughout our practice we have observed a number of inaccurate, unhelpful assumptions around student knowledge and awareness of online risks as they transition to higher education. Terms such as 'digital natives' (see Prensky, 1991) are extremely problematic, stereotyping a whole generation who are, in some inexplicable way, digitally aware simply as a result growing up in an increasingly digital society and being born after an arbitrary year.

Prensky's Digital Native idea comes from an article that proposes a theory where because someone was born in an era where digital technology was ubiquitous, they had some inbuilt ability to engage with it with capabilities that are missing from previous generations generalized as digital immigrants. While this crude generalization is now widely debunked (for example Helsper and Eynon 2010), its use still pervades in popular discourse.

We have certainly attended seminars and workshops around digital literacies and safeguarding within the higher education sector where senior speakers from government and regulators have unhelpfully spoken of younger generations being natives capable of navigating the digital world without further support. To paraphrase one presentation:

> *"They're digital natives, it comes naturally to them".*

The term, when unchallenged, has become a taken-for-granted assumption and we frequently hear it in policy discussions and conferences related to students' use of technology. It is mainly used in one of two ways – firstly, as a way to imply blame:

> *"They're digital natives, they should know about this sort of thing"*

Or it is used to deflect responsibility:

> *"I'm not a digital native like they are, they know more than me".*

Brown and Czerniewicz (2010) amongst others, are also highly critical of the concept as such terminology hides inequalities in digital experiences. Furthermore, given that *Digital Native* ties in with the concept of *Millennials* (born between mid 1980s and early 2000s) and *Generation Z* (late 1990s - approximately 2015) this is not a term that could simply be applied to children and young people now – it is both unproven and now obsolete when we are concerned with the online safeguarding of young people in 2021. If we were to engage with this many adults would now be considered digital natives, including some who are claiming there are cultural challenges in online safeguarding because of digital natives.

Yet we know that stark digital divides remain across socio-economic, gender and geographic clusters and there is, in reality a considerable diversity in young people's ability to use and their knowledge of the internet and online forums and their opportunities to access and interact online.

What is clear from wider evidence, and again something we have observed in many policy discussions around institution's duty of care, is that, again arguably as a means of deflecting responsibly, there is a very mistaken assumption across the HE sector that students receive online safety education in schools and that they therefore, transition to university equipped to deal with issues of online harassment and abuse with no further need for awareness raising or education around critical digital literacies.

V. The State of Online Safeguarding in the UK Higher Education Sector Pre-COVID

As we have discussed above, our experience in researching this area for considerable time, as well as working in the UK higher education sector, meant that our expectations around online safeguarding across universities was weak even before COVID-19 focused our minds on the welfare risks associated with online delivery. While the Warwick case brought these concerns into focus, we, as academics, wished to look beyond media reporting for a more rigorous evidence base to highlight our concerns. As such, we conducted a detailed collection of evidence around the state of the sector in 2019 that helps us understand why online harms were not tackled effectively during lockdowns.

The core of this evidence-based centers upon Freedom of Information requests[1]. The Freedom of Information Act 2000 (UK Government 2000) in England, Wales and Northern Ireland and the Freedom of Information Act (Scotland) 2002 (UK Government 2002) allow us to request information from public bodies (and UK universities are public bodies) and expect a response within a reasonable time period (normally 20 working days) (Information Commissioners Office n.d.). Since introduction of the acts public bodies have to provide a means for members of the public to place requests for information, and we used these access mechanisms (generally an email address) to send a list of questions to all UK higher education institutions, ultimately in two tranches. The first request submitted was concerned with policy and recording. We initially wanted to discover whether universities had clearly defined policy on online harassment, abuse and hate speech because it is, arguably, impossible for an institution to respond in a coherent and uniform manner to incidents without clearly defined policy for all staff to follow. Additionally, we wished to discover senior management and board level responsibilities for safeguarding and the frequency of recorded incident related to online abuse in institutions.

We divided our exploration into two requests – one which focused upon policy, senior management responsibilities, and scale of online abuse within the setting:

- *Your university polic(ies) addressing how the institution tackles online abuse (including image-based abuse and online harassment) or hate speech online in the student body.*
- *The name of the member of your university executive team directly responsible for student safeguarding.*
- *The name of the member of your university governing body/board directly responsible for student safeguarding.*
- *Details of how students can report incidents of online abuse (including image-based abuse and online harassment) or hate speech online in your institution.*
- *The number of student disciplinaries where online abuse (including image based abuse and online harassment) or hate speech online was a factor per year for each academic year from 2015-16 to 2017-18.*
- *Number of reports made to the police where online abuse (including image-based abuse and online harassment) or hate speech online was a factor per year for each academic year from 2015-16 to 2017-18.*

A follow up request was sent in September 2019, in order to address some of the questions raised by the responses we had received in the first response, and also to focus more specifically on the training of staff and work with external bodies:

- *Does your university provide any training to staff on online harassment/abuse?*
    - *If so, is this dedicated training, or is it covered in more generic training on harassment and bullying?*
        - *If it is generic training, please outline what it covers specifically about online harassment/abuse?*
        - *If this is specialist training, what aspects of online harassment/abuse are covered?*

[1] See https://www.gov.uk/make-a-freedom-of-information-request

- *If you do provide training, is the training you provide to university staff about online harassment/abuse mandatory for all staff? If not, which staff are expected to undertake the training?*
- *Does your university provide training to staff who investigate student complaints on online harassment/abuse? Is this training mandatory?*
- *Does your university provide training to staff who investigate staff complaints on online harassment/abuse? Is this training mandatory?*
- *Does your university provide training to any staff on handling disclosures of online sexual abuse?*
    - *Does this training include handling disclosures by both students and staff?*
    - *Does this training include handling disclosures of online child abuse, e.g. the possession/manufacture/distribution of child abuse images, online grooming, sexual communication with a child?*
    - *Are there any awareness raising activities for students related to possession of child abuse images?*
- *If a student or staff member reports a hate crime with an online element (e.g. racism, homophobia) is this recorded as a specific hate crime or online harassment/bullying/abuse or both?*
- *How does the university record complaints that involve both online and offline harmful/offensive behaviour (for example the in class and online sexual harassment of a student)? Will the online aspect of the adverse behaviour always be recorded?*
- *Does the university have a relationship with specialist provider(s) that deals with online harassment which it can take advice from and refer victims to for support?*

While the full reporting of the findings is available elsewhere (Phippen and Bond 2020) there are a number of key aspects worthy of exploration in this chapter, particularly when considering university preparedness for tackling student welfare in online settings, and the support available for victims.

By way of illustration of the awareness of online safeguarding, or safeguarding in general, across the university sector, as early response to our first request illustrated this clearly. We were asked very early in our explorations to clarify what we meant by student safeguarding because it seemed they did not believe that, as a university, had any safeguarding duties due to the lack of minors in their care:

> *We have been asked to clarify your definition of "student safeguarding" as the University would normally use the term "safeguarding" concerns raised about individuals under the age of 18.*

We were a little shocked, but perhaps disappointingly not too surprised, that it is the belief of this HEI organization that safeguarding is normally only a matter for those below the age of majority. We reminded the institution that there are statutory requirements for adult safeguarding well established in law in the 2014 Care Act (UK Government 2014) and the university sector had been guided by the member organization from UK universities (Universities UK) 'Changing the Culture' report published in 2016 (where safeguarding is mentioned 8 times) (Universities UK 2016). Another interesting response, which provide a great deal of food for thought, came from a refusal to respond based upon a "section 12 exemption" (UK Government 2020) – essentially it is written into the legislation that if it takes the organization an unfair amount of time to respond, they do not have to. In this case the response stated:

> *We estimate that to determine whether we hold the data in relation to questions 5 and 6, 'number of student disciplinaries' where online abuse (including image based abuse and online harassment) or hate speech online was a factor', then separately, 'number of reports made to the police where online abuse (including image based abuse and online harassment) or hate speech online was a factor' for the three years requested, then to locate, retrieve, and extract that information would take longer than 18 hours to complete. The primary reason for why the appropriate limit would be exceeded, is that the information requested is not recorded centrally in an easily searchable, aggregated format. In order to locate the data requested we would have to manually interrogate records of each Student Halls Wardens, of which there are ten, whose records are not held in a central easily searchable aggregated format, to identify whether a complaint or disciplinary matter had online abuse or online hate speech as a contributory factor to the allegation(s), and then whether the incident was reported to the police.*

A very clear response that illustrated the institution had no central recording of harassment and abuse incidents, and could therefore have no means of determining the scale of the problem among their student body. However, in total we received responses from 130 institutions. In the first part of the request, we asked about policy. Having effective policy is a fundamental part of safeguarding – if an institution does not have policy in place, how can they have a uniform way in which to address an issue. Furthermore, lack of policy would suggest that an institution had not considered the issue in question.

We were specific in the request that the institution should tell us where they believed they addressed online abuse and harassment. While universities do publish policies on their websites, we wanted to be told by the institution how they addressed this issue, rather than searching through the policies ourselves (which was suggested by a few respondents!).
In our responses, we saw incredibly varied and inconsistent practice across the sector. Of those who responded to the request there were a total of 21 types of different policies which were identified as addressing how the institution tackles online abuse (including image-based abuse and online harassment) or hate speech online in the student body. The main policy used by universities related to student discipline/code of conduct or regulations with over 80 universities stating that this is was their main policy. Just over 40 HEIs reporting having a specific Bullying and Harassment Policy and 30 stated that online

harassment and hate crime were covered by their Dignity and Respect at study policy. Just over 20 had a Social Media policy and 20 said it was addressed it their IT regulations and Acceptable Use Policies. In total we were send 266 policies from our 130 responding institutions. We received at least one policy from 121 HEIs, suggesting that the other 8 did not believe they had policy to cover this (discounting the 4 refusals).

In order to ensure that we could analyze the policies in a consistent manner, we ran a keyword search algorithm on them. We felt this was more consistent than reading through them in the first instances ourselves, as we many have missed some coverage. The keyword list we used was:

> *['online', 'social media', 'harassment', 'online harassment', 'online abuse', 'hate speech', 'hate crime', 'digital', 'cyberbullying', 'cyber bullying', 'online bullying', 'pornography']*

We found that, in general, there was little coverage of our keyword set in these policies, which would suggest that overall, these policies (somewhat surprisingly given the nature of the policies, i.e. student conduct and bullying and harassment) had little coverage of online abuse and harassment. Almost 60% of the policies provided by institutions where they claimed coverage of online harassment and abuse had no mention of "online" whatsoever. While "harassment" is well covered, if we consider "online harassment" as a distinct abusive behaviour, it is hardly covered at all, as is hate speech or hate crime. While "social media" does receive coverage in just over 50% of policies, a lot of those policies relate to social media conduct (i.e. "think before you post") rather than the use of these platforms to abuse or harass. Given our intention for this request to for institutions to tell us how they coverage online abuse and harassment in their policies, therefore giving them the best opportunity to provide this evidence, it is concerning to see that in 60% of cases policies the institution believed to cover online abuse actually had no mention of it.

In response to being asked for the name of the member of a university executive team directly responsible for student safeguarding 110 of the 130 HEIs who replied had a named person responsible but fifteen did not and five refused to respond to the question. Interestingly a number of replies also stated that an HEI they did need to have named people responsible for safeguarding as the rather alarming example below illustrates:

> *"The University is not obligated to hold these designated roles. As we are a Higher Education Institution this places us in a different position to school/college institutions and we are not required to designate specific person(s) to be directly responsible for safeguarding."*

Which would illustrate that, for some institutions, without a statutory requirement, they do not believe this is something they need to do. Again, very concerning that a university does not consider having a senior manager to hold responsibilities for safeguarding, given student welfare should be a fundamental part of university support.

Equally concerning was the response regarding board membership responsibility for safeguarding. Only 43 had a named member of their university governing body/board directly responsible for student safeguarding. While five HEIs refused to provide an answer to the question, 81 reported that they did not have a named person on the university board directly responsible for student safeguarding. Given that university boards/governing bodies are supposed to hold senior management in an institution to account without a board level responsibility, how can student safeguarding be an accountable activity? Without a lead on the board, it seems unlikely that sufficient challenge could be made, which presents another reason why the sector is currently not on the surest of footings when it comes to safeguarding in general and online safeguarding in particular.

We also asked HEIs to provide details of how students can report incidents of online abuse (including image based abuse and online harassment) or hate speech online in their institution. Like the findings in relation to the policies, we found a wide variety of responses. 31 HEIs had introduced anonymous online reporting as a means, in their view, to be able to support students who are victims of abuse.

While we can appreciate some of the rationale for anonymous reporting (i.e. this is a sensitive topic and some student might not wish to provide personal information) we would, from a student centric and organizational risk perspective, suggest that anonymous reporting are not an effective safeguarding measure.

If student reports abuse anonymously, there is little an institution can do to support the student other than to respond and hope that a discussion is established. If, for example, a university receives an anonymous report stating:

"There are images of me being shared across my year group"

There is little the responder can do without specific detail. While some generic advice such as "report this to the police" might be possible, advice will be very non-specific. While anonymous reporting systems may appeal because they have a low draw on resource and provide a means of data collection, there is much to consider in terms of victim support and data protection. At best, any institution using anonymous reporting must have an underlying policy on data processing for it to be legal (and we were not provided with any policies that covered anonymous reporting). A policy should consider accusations and vexatious claims, and define how data will be stored and what approach is made for notification. We would suggest that anonymous reporting should only be used as part of a larger suite of reporting tools. Given the responses to the questions about volume of reporting below, we see no different between those who use anonymous reporting and those who do not, which would suggest the aim to better understand the prevalence and nature of online abuse is not being met.

In terms of the volume of disclosures around online abuse, responses were not very helpful. Firstly, there were a reasonably large volume where online incidents are not recorded at all, and there are a number who refused due to resource issues in finding this information. This would suggest no central recording system where this information is easily accessible, which is a concern of itself. In general, universities returned very small numbers of recorded incidents, which, given the lack of policy or consistent reporting should come as little surprise. If an institution has no policy around tackling online incident, it should come as no surprise that there are not many recorded disclosures. Given students bodies of several thousand in a lot of institutions, having less than five recorded instances of online abuse in a year seems highly unlikely, which then raises concerns around whether students are reporting this abuse and have routes for disclosure, and, if they are reporting it, is it being recorded accurately?

Our first set of responses, to the first request, gave us a number of causes for concern:

- Ineffective policy
- Poor reporting routes
- Poor recording of incidents

All of which would suggest safeguarding systems across the sector are not equipped to deal with online abuse. The subsequent request, which centered on training, nature of training, and working with external agencies, gave us more detail about poor practice across the sector.

In total for the second Freedom of Information request we received 106 responses. The information provided allowed us to probe more deeply into sectoral knowledge around online harassment, abuse and hate speech, and also attempted to gain a deeper understanding of why recording incident levels of online abuse in the sector seem so low.

Alongside policy, training is an essential part of the foundation for effective support of students who might be affected by online harassment – without effective training and policy an institution cannot hold any confidence that it is capable to supporting students who become victims of online abuse, they have neither a documented response, nor knowledgeable staff to support them.

Looking initially at training provision 54% of respondents claimed some level of staff training around online abuse. This means almost half of the institutions in the sector provide no training. Of those who do provide training, the vast majority (96%) said that online abuse, harassment and hate speech is tackled within “generic” training. When probed about the nature of this training, it ranged from IT induction training to instruction related to equality and diversity. Some institutions also covered these issues in bullying and harassment training. We had one respondent reply to say there was no need for training on online abuse because it was the same as the offline equivalent.

The nature of coverage was generally in the form of examples and scenarios, and these examples could range from anything to emails as harassment to social media abuse. There were no institutions who provided training as part of wider “generic” instruction that said they covered things like image-based abuse (sometimes referred to as revenge pornography), understanding legal thresholds or issues such as online stalking. Moreover, of those who did provide training, only 65% delivered this as mandatory training. Therefore, we could be confident that only 30% of institutions responding gave training to all staff on any aspect of online abuse or harassment.

Exploring more deeply into the level and nature of training related to dealing with online abuse in higher education institutions, we asked some more specific questions around the more extreme side of abuse – namely, sexual abuse, grooming and indecent images of children. Therefore, we might expect, in a university’s duty of care for student welfare, that those who support students would be aware of these issues and how students might be supported. One respondent claimed formal training was not necessary because “Training occurs through shared experience and knowledge within the Student Support and Wellbeing team". However, we would doubt the effectiveness of a peer sharing scheme without a formal element for covering evolving issues such as legal precedent and case law.

Responses to the requests would suggest that the majority of HEIs do not provide any training, with 57% saying none was provided. Of those who did provide training, 67% of respondents said this covered dealing with disclosures from both staff and students, whereas the remainder (33%) only provided instruction regarding handling disclosures from students.
The recording of incidents was a section added to the second inquiry because we had such low results in recorded incidents in the first one. We wanted to understand how universities recorded reported incidents to consider whether this was an issue in the accuracy of the nature of incidents reported. It was clearly apparent that this was the case, with few respondents saying they would specifically categorize a report as online abuse in their reporting systems for both online harassment/abuse and those complaints that might be complex but contained an online element. The vast majority of respondents said they did not categorize (60% for online abuse, 77% for complex complaints) these reports, and around 16%/14% said they would record as both online and the more general categorization (for example harassment or hate crime). Only around 5% of respondents said they would specifically record online elements.

One respondent said "we don't distinguish from other disclosures" and four who did not categorize incidents stated somewhat confusingly that categorization was not needed because they used anonymous reporting. What was clear from the myriad of responses, however, was that it is unlikely institutions accurately categorize complaints to a level where they can determine prevalence of online to offline incident, which might go some way to explain low levels of reporting of online incident from the initial FOI inquiry.

We also had, in response to the question around categorization, two respondents referring to the Office of the Independent Adjudicator for Higher Education (a government agency that provides students with a route to complain about their treatment by a university) guidance on good practice for handling student complaints and academic appeals (Office of the Independent Adjudicator 2016). This guidance provides no indication of how one might categorize incidents, so it seems strange to refer to it in a question on categorization. Again, without effective categorization of incident, we are unsure how a university might better understand opportunities for improvement or training.

In the final part of the second inquiry, we asked whether universities worked with external bodies, to whom they could learn or refer student victims. We were unsurprised to discover that the vast majority (73%) of respondents had no links to external agencies. Of those who did (27%), there were a variety of links reported, such as police, sexual assault referral units, domestic violence NGOs, mental health support, Rape Crisis, the Revenge Porn helpline and Victim Support. Interestingly the majority of those reported had little specialism around online abuse.

VI. Online Harms in the COVID-19 Pandemic

Our Freedom of Information based investigation of the sector in the UK related to support for students in addressing online harms and abuse gave us little confidence that institutions were doing this effectively. We had received evasive responses, responses suggesting student welfare was not their concern, and considerable evidence to suggest that students had few routes to disclose abuse and obtain support, given the dearth of policy in the sector.

Therefore, it came as no surprise to us that there was increased evidence on incidents across the sector during lockdowns. Anecdotally, as two academics working across the sector in the UK, and sometimes in demand to advise on such issues, it appeared that there was increased concern around online abuse during lockdowns and online delivery, and increasing numbers of student disciplinaries being dealt with by the sector related to online abuse. As a demonstrate of poor safeguarding practice, this is typical. While an institution might not deliver any education around online abuse, or have policies in place, or have disclosure routes for students, they have no means of tackling these issues until it becomes sufficiently serious to result in a student disciplinary. At this point the disciplinary will be convened by student support services who have received no training about online abuse, and have no policy to guide them in how to respond, and have disciplinaries chaired by senior managers who, too, have received no training so bring nothing other than their own value biases as a result of their own use, or lack of use, of digital technology in their lives.

One thing evident from both cases we were asked to advise upon, and also those covered in the media, was a lot of these abuse incidents arose not just from the behaviour of students, but also the lack of knowledge of staff to deal with them. One thing we observed very early in the lockdowns and a move to online delivery was that staff we rarely provided with any training or support in using these new online delivery platforms. There seemed to be an assumption that, because online systems are used for some aspects of university activity, such as email for communication and learning platforms for the dissemination of teaching materials, everyone would somehow intuitively be able to move to fully online delivery without the need for even the most basic of training. What became apparent, particularly from those incidents that were very much facilitated by the delivery mechanism, was that there was as much need for cybersecurity knowledge than student support. Let us take, for example, the tales of “Zoombombing” in the sector, something that was quickly attracting the attention of the media early in the pandemic (for example Batty 2020).

In these cases, to generalize, a teaching session would be taken over by a student (or unauthorized attendee) who would begin to play pornographic material on the screen. Or, as perhaps a less extreme form of abuse, an attendee would start playing pornography on another device so all of the classroom could hear it, and the host of the class could not see where it was coming from. The response in institutions and the media was that it was the technology itself that was not fit for purpose. Surely, the technology should be able to prevent the authorized access and prevention from playing such material? How could the platform provider allow this to happen? The view of senior management was that “We pay a high premium for this product; the platform should make these sessions secure”.

And, of course, it could. But it required a knowledgeable host to be able to manage it. In most mainstream platforms (which we should remind readers are were not developed for the classroom, but for remote meetings) the host of the session can ensure that they are the only one who can manage what goes on the screen. Equally, they should be able to mute all attendees, and see if anyone is unmuted. They should, of course, also be able to eject and block misbehaving attendees and ensure the session is password protected so only invited attendees can join.

While the appropriateness of the use of a video conferencing/meeting platform for teaching remains one to debate, it is the case this is all manageable with a trained and knowledgeable host. However, this cannot do this automatically, it requires knowledge on the part of the host to set up the access control and manage the session. The platform cannot, of itself, prevent the misbehavior on a participant in a session. And we are very aware that in the rush to move teaching online, there was little time or investment in developing the knowledge of the academic staff required to deliver the sessions. There is, as we observe frequently, an assumption that users of digital technology have some implicit capacity to learn through osmosis. You have a PIN on your mobile device? Well of course you will understand the need for access control on video conferencing platforms!

In the cases such as zoombombing, the exposure to upsetting and harmful content comes as a result of the failure of the operate to control the learning platform. Students are exposed to potential harm as a result of being in a session they are expected to attend. Yet can we also readily blame the untrained academic. Surely there is an institutional duty of care here? While we are sympathetic to the rapidity in which things moved online during the pandemic, it is not sufficient to assume we are all sufficiently technically capable of using the technology in a safe manner.

If we consider a separate incident, a hypothetical based upon a couple of incidents on which we were asked to advise - a student is subject to persistent sexual harassment and hate speech on a Discord server the students have implemented to support interactions on their course. Discord is a communication platform that allows users to set up groups so that they can work and discuss together, even when physically isolated. In this scenario, the server is not hosted by the university but the academic team are aware it has been set up and was, until this point, keen to encourage students to use digital platforms to interact.

In this case the student makes a complaint to the programme leader about the abuse, and asks them to intervene. The first thought of the programme leader might be “we didn’t provide the platform, its not our problem”. The student has, by this stage, looked up policies on the university website to see how the institution will support them as a result of being subject to harassment facilitated in a university virtual classroom. Then see nothing there, and the attitude of the programme manager is one panic, rather than the consistent application of policy. We would hope that they would soon realize that student welfare is their concern, and did they have appropriate routes for disclosure and clear and transparent policies around sanctions for online abuse? It would be extremely unlikely in this situation that there would be a technical solution to this abuse. However, the fact that the university encouraged the use of a platform they could not control, for informal learning within a degree course, without any policy around how to address abuse or route for disclosure for the student, would suggest they could be found negligent in preventing the abuse.

There is a growing view in the policy space (as we can see if we spend any time with the UK Online Safety Bill [ref]) that because the digital environment is where “online harms” take place, it should be the providers of these environments who should ensure harm cannot take place. We can also see this within the Higher Education sector – the afore mentioned security teams challenged on not shutting down attacks or invitations to tender specifying a network provider should “prevent harm” on the networks provided. This is, again, an absolving of responsibility on the part of the institution. The platforms will generally have tools to address access control, participant management, and reporting routes for abuse. However, they will not work without knowledgeable staff and students.

We have also seen an increase in ransomware attacks across the UK higher education sector and, again, this should not be surprising, given the importance of having online systems available to all stakeholders. Generally, these attacks are triggered by phishing emails and, anecdotally, this has focused the sudden need for great cybersecurity awareness by staff and students. Again, an entirely reactive approach to something that could have been foreseen. We would imagine there are similar conversations across the sector – poorly resourced and put-upon cybersecurity managers are asked “how could you let this happen!?” after spending many years arguing that they and their administrative team of two cannot possibly shut down all of the threats that appears in the inboxes of the thousands of staff and students and across campus networks.
In increasingly digital higher education spaces, it can no longer be left to the technology to mitigate online risks across campus. It comes as no surprise that there seem to be many institutions now sending out online training around “ransomware prevention”. However, we would question whether a half hour online course is sufficient to understand the role the end user plays in cybersecurity and online harm. These are “whole institution” issues requiring education and awareness across all stakeholders and leadership at the top levels of the organization.

Technology can only ever serve as tools to support the systems that need to be in place to mitigate cyber-risk in organizations and provide students and staff with the means to disclose abuse and gain support from an institution. While filtering against illegal content will prevent access on institutional networks, there are freedom of expression challenges to be met if similar tools are to be used for “legal but harmful” content. Monitoring can identify abuse taking place on networks but it is by no means a perfect system. They will generally only trigger based upon keywords or phrases, and if applied to strongly will intervene to readily in innocent discourse. And while the digital tools of cybersecurity, such as anti-virus software, firewalls and intrusion detection systems, will all help mitigate risk of cyber-attack, they will do little to prevent a member of staff or a student hand over their login details via a phishing attack.

VII. The Duty of Care for Institutions

A term that is becoming increasingly de rigueur in the online safeguarding world, and one we have made liberal use of throughout this chapter, is “Duty of Care”. It is throughout the UK Online Safety Bill (UK Government 2021), which is currently in draft before UK parliament, and there is much discussion, without underpinning case law, what this duty of care might look like in the higher education sector. It is unquestionable (regardless of responses from Freedom of Information requests) that a university enters into a contract with a student to provide a service, and the student is within their rights to expect the service to be delivered in a safe manner. For example, one might argue that abuse during an online class, using a platform provided by the institution, means that the university is liable or negligent.

The concept of negligence, in law, is a complex one and is frequently debated in the courts. There seems to be little attempt to define or delineate whether this online duty of care aligns specifically with the broader legal concept of duty of care, and its relationship with the tort of negligence. Is the duty of care in the white paper being defined as a form a negligence, and if so, how might the company be able to demonstrate due diligence or protect itself from vexatious claims of harm? Negligence is the subject to much legal debate and is certainly not getting any less complex, as rather beautifully claimed by Markesinis & Deakin's (2012) Tort Law, a seminal legal text:

> *The experience of the last thirty years or so if anything, suggests a dialectical process of evolution with many, often inexplicable, tergiversations.*

Nevertheless, the fact that Warwick University was subject to a negligence claim as a result of their dealing with the high profile group chat scandal suggests that if and when case law is established institutions would do well be to cognizant of their duties and be able to be in a position to demonstrate due diligence.

While we feel this it would be unreasonable to argue that a university is liable for any abuse that occurs on platform provided by the institution for student learning, either formal or informal, we would argue that demonstrating duty of care is concerned more with having effective policies in place, supported by disclosure routes and well trained and responsive staff. As we have discussed above, the concept of safety is a utopia that is unachievably in the online world. However, an institution can mitigate the risks and provide sufficient infrastructure and practice to support individuals in becoming resilient and being able to find support and resolution, with appropriate sanctions to the abuser, should they become subject to abuse.

For example, we were recently made aware of a member of the academic community who, excited to see their class on screen, decided to take a screen grab of each member of the group, which was shared further. While this was clearly an act that is done for all of the best intentions, we need to bear in mind that students have not consented to their images being shared, and the image capture might contain personal items or details that could result in abuse.

While we moved swiftly to online delivery, and learning what works most effectively, sometimes the thrill of the technology can make us neglect fundamental safeguarding principles. While it is perhaps a novelty to see all of our students faces on the screen, we need to be mindful that, in contrast to a face-to-face classroom scenario, students will be in private spaces and that privacy should be respected. While it is in the gift of the student to switch off their camera, we should reflect upon whether there is any necessity to expose students' privacy in this way with online delivery in the first place.

As such, this would be an unwise thing for a “cyber aware” academic to do. However, they might legitimately argue that, without training or awareness of such, how might they be expected to know this? The institution has instructed them to use on online platform that is, arguably, not best suited for teaching. Therefore, there is a realistic expectation of training or support at the same time.

By way of mitigation, a useful practice might be the consensual recording of classes, but this should be alongside clear policy around data retention and safeguarding rationale. Clearly the recording of a class is important as a means to evidence abuse that might occur, but also to protect the member of staff for vexatious accusation of inappropriate behaviour. This is particularly important for smaller, or one-to-one, meetings with students. Moreover, it is important that institutions should recognize that while online delivery changes how we might interact with students, it does not change the fundamental relationship with them in terms of ensuring a safe environment to study, clear routes for disclosure should an incident occur and transparent and consistent disciplinary routes when dealing with abusers.

However, our work has highlighted that this is currently a sector in reactive mode. While the move to online delivery has focused the minds of some regarding online safeguarding, and it is clearly now on the radar of senior management, there is still much to do to ensure we do have a sector that can demonstrate its due diligence and strongly evidence it takes its duty of care seriously.

VIII. What Can Institutions Do?

In bringing this chapter to a close, we should consider practical steps that institutions can adopt. It is unquestionable that COVID-19 has accelerated our thinking about online and hybrid delivery models, but the rapidity of adoption of technologies has not been matched with institutional responses to the increased potential for online abuse and institutional liability. We have shown, through our own empirical work, the universities were not in a good place to support students at risk of online abuse prior to lockdown, and it has not improved since. In a post-COVID higher education environment, where hybrid learning is not just a possibility but an expectation, universities can no longer hope that this will not happen to their students.

Online abuse *is* different and cannot merely be dismissed as a medium by which abuse and harassment occurs. As we have seen through this lockdown year, and before, it facilitates far great geographic reach than abuse on campus, and can be maintained through multiple platforms and devices. In essence, there is no escape. Furthermore, the "pile-on", when an abuser encourages others to participate in online abuse, is no something that can be easily replicated in an offline setting. We know, through our many years research in this area, that online abuse is often dismissed as "banter" – something that should be tolerated as an expected aspect of engaging with online platforms. By considering online abuse to merely be a facet of harassment in its more traditional sense does nothing to raise awareness of these issues in the sector, appreciate the severity of impact or make universities any more mindful to take online abuse on their campuses, whether they be physical or virtual, seriously.

We have mentioned the lack of knowledge around online abuse and harassment by the student body, and have gone to great lengths in the past to criticize lazy assumptions of the "digital native" arriving at university equipped with the knowledge and resilience to tackle all of the potential online harms that might beset them in early adulthood. With a dearth of effective relationships and sex education in schools, student do not need "awareness training", they need *education* embedded into their studies to appreciate how these issues affect their lives now, and in the future. At all life stages, whether school, university or the workplace, there seems to be a view that "someone else" should provide the necessary knowledge and understanding to be able to recognize abuse and how to respond to it. This is not something that can be addressed with an optional online training video and a multiple-choice quiz, it needs to be robust education delivered by experts, and it is crucial that it takes place from a risk mitigation and harm reduction perspective, rather than a preventative one. A fundamental aspect of this has to be cybersecurity knowledge. A student who understands cybersecurity basics such as good password practices, the management of their devices and access control is far less likely to become a victim of identity theft or online abuse, as their digital assets will be better protected. The same is true of staff – we cannot assume, because they already own a mobile phone and use social media, that they are somehow magically capable of managing an online classroom without some form of training and support.

IX. Footnote

As part of our work in this area, in 2019 published a toolkit for universities (https://www.uos.ac.uk/sites/www.uos.ac.uk/files/Higher-Education-Online-Safeguarding-Self-Review-Tool%202019.pdf) to allow them to review their current policy and practice, and how they might develop effective strategies for online safeguarding. While there are some UK legal specifics, the majority of the tool is portable and freely available for anyone to use under a creative commons license.

X. References

Batty, D. (2020). *Harassment fears as students post extreme pornography in online lectures.* The Guardian. Available from: https://www.theguardian.com/education/2020/apr/22/students-zoombomb-online-lectures-with-extreme-pornography. [Accessed September 2021]

BBC News (2018). *Warwick University students protest over rape chat probe.* Available from: https://www.bbc.co.uk/news/uk-england-coventry-warwickshire-47147269 [Accessed September 2021]

BBC News (2019). *Inside the Warwick University rape chat scandal.* Available from: https://www.bbc.co.uk/news/uk-48366835 [Accessed September 2021].

Bond, E. (2014) *Childhood, Mobile Technologies and Everyday Experiences* Basingstoke: Palgrave.

Brown, C., & Czerniewicz, L. (2010). Debunking the 'digital native': beyond digital apartheid, towards digital democracy. *Journal of Computer Assisted Learning, 26*(5), 357-369.

Deakin, Simon F. and Johnston, Angus C. and Markesinis, Basil S., *Markesinis & Deakin's Tort Law - 7th Edition* (October 18, 2012). Oxford University Press, 2012. p. 99

Helsper, E. J., & Eynon, R. (2010). Digital natives: where is the evidence?. *British educational research journal, 36*(3), 503-520.

Henry, N. and Powell, A. (2016) *Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research.* Trauma, Violence and Abuse, Vol. 19(2) pp. 195-208

Hess A (2014) Why women aren't welcome on the Internet. *Pacific Standard*, 6 January available online from: https://psmag.com/why-women-aren-t-welcome-on-the-internet-aa21fdbc8d6

Information Commissioner's Office (n.d.). *What is the Freedom of Information Act?* Available from: https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/ [Accessed September 2021]

Office of the Independent Adjudicator (2016). *The good practice framework: handling student complaints and academic appeals.* Available from: https://www.oiahe.org.uk/media/1859/oia-good-practice-framework.pdf [Accessed September 2021]

Phippen, A. (2016). Children's online behaviour and safety: Policy and rights challenges. Springer.

Phippen, A. and Bond, E. (2020) Online Harassment and Hate Crime in HEIs. Available from https://www.uos.ac.uk/sites/www.uos.ac.uk/files/FOI-Report-Final-Jan-2020-rgb_0.pdf [Accessed September 2021]

Poland, B. (2016) Haters: Harassment, Abuse and Violence Online. Potomac Books.

Powell, A.; Scott, A. J and Henry, N. (2020) Digital harassment and abuse: Experiences of sexuality and gender minority adults in European Journal of Criminology Vol. 17 (2) pp. 199–223 Vol. 17 (2)

Prensky, M. (2001). Digital natives, digital immigrants part 2: Do they really think differently?. *On the horizon*.

Reid, A. (2016) *Trolls and Tribulations: One-in-Four Canadians Say They're Being Harassed on Social Media*. Available from: http://angusreid.org/wp-content/uploads/2016/10/2016.10.04- Social-Media.pdf [Accessed September 2021).

UK Government (2000). *Freedom of Information Act 2000.* Available from: https://www.legislation.gov.uk/ukpga/2000/36/contents [Accessed September 2021]

UK Government (2002). *Freedom of Information (Scotland) 2002.* Available from: https://www.legislation.gov.uk/asp/2002/13/contents [Accessed September 2021].

UK Government (2014). *The Care Act 2014.* Available from: https://www.legislation.gov.uk/ukpga/2014/23/contents/enacted. [Accessed September 2021].

UK Government (2021). The Online Safety Bill Draft 2021. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf. [Accessed September 2021]

Universities UK (2016) *Changing the Culture Report of the Universities UK Taskforce examining violence against women, harassment and hate crime affecting university students.* Available from https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2016/changing-the-culture.pdf [Accessed September 2021]

Veletsianos, G.; Houlden, S.; Hodson, J. and Gosse, C. (2018) *Women scholars' experiences with online harassment and abuse: Self-protection, resistance, acceptance, and self-blame*. New Media & Society Vol. 20(12) pp. 4689–4708

Professor Andy Phippen is a Professor of Digital Rights at the Bournemouth University, UK and is a Visiting Professor at the University of Suffolk, UK. He has specialised in the use of ICTs in social contexts and the intersection with legislation for over 15 years, carrying out a large amount of grass roots research on issues such as attitudes toward privacy and data protection, internet safety and contemporary issues such as sexting, peer abuse and the impact of digital technology on wellbeing. He has presented written and oral evidence to parliamentary inquiries related to the use of ICTs in society, is widely published in the area and is a frequent media commentator on these issues.

Professor Emma Bond is Pro Vice-Chancellor Research and Professor of Socio-Technical Research of Suffolk at the University.
Emma is a Senior Fellow of the Higher Education Academy and has over 20 years teaching experience on social science undergraduate and post-graduate courses including PhD and extensive research experience focusing on online risk and vulnerable groups; image-based abuse (sexting and revenge pornography); online harassment; domestic abuse and sexual abuse.