University of Suffolk

Online Harassment and Hate Crime in HEIs – report from FOI

By Professor Andy Phippen and Professor Emma Bond

January 2020

Contents

Introduction

Student safeguarding is a well-established responsibility for higher education in the UK. However, responsibilities for online safeguarding are only recently becoming recognised across the sector. "Illegal and unacceptable content and activity is widespread online, and UK users are concerned about what they see and experience on the internet"[1]. As the recent study by Davidson et al. (2019: 1) suggests[2]:

> *The development of email and social media platforms has changed the way in which people interact with each other. The open sharing of personal data in public forums has resulted in online harassment in its many forms becoming increasingly problematic. The number of people having negative online experiences is increasing, with close to half of adult internet users reporting having seen hateful content online in the past year.*

According to Ofcom (2019)[3] half of adult internet users in the UK report that they are concerned about online content, and nearly half (53%) report seeing hateful content online in the past year (with 14% reporting that they had seen this 'often'). Online harms, well acknowledged in the compulsory educational sector (as exemplified by the Ofsted education inspection framework (2019)[4] and the Department for Education's (2018) *Keeping children safe in education: Statutory guidance for schools and colleges*[5]) do not cease when young people enter into late adolescence and early adulthood. The launch of the Universities UK (UUK) 'Changing the Culture' report in 2016 exposed the experiences of violence against women, hate crime and harassment affecting university students and called for further action to specifically tackle online harassment and hate crime. However, in spite of a duty of care accorded to universities in the UK to act reasonably in students' best interests, to protect their well-being and provide appropriate support, there has until very recently been a dearth of guidance in relation to current practice and regulation around online safety within the higher education sector. To address this discrepancy, UUK launched their Tackling Online Harms and Promoting Online Welfare report[6] in September 2019.

Online harassment can have a lasting impact on those who are victimised. Effects range from mental or emotional stress to financial loss, and in some cases difficulty in securing employment and housing (Davidson et al. 2019)[7]. Furthermore, in the last few years the press has reported a number of high-profile cases of online abuse, harmful and hateful content, as well as risky online behaviour that has left the HE sector reeling (for example, [8] [9] [10]). As the findings in this report suggest, universities are uncertain how to best respond, and many university staff remain unsure of how best to support and protect victims of abuse, how to sanction offenders, or how to manage the reputational risks to their institutions. Other than the recently published guidelines by UUK, it is clear that across the sector there is little help and guidance available. Moreover, there are a number of inaccurate and unhelpful assumptions around student knowledge and awareness of online risks as they transition to higher education. Terms such as

1 Online Harms White Paper (2019: p. 5) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

2 Davidson et al. (2019). Adult Online Hate, Harassment and Abuse: A Rapid Evidence Assessment https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811450/Adult_Online_Harms_Report_2019.pdf

3 https://www.ofcom.org.uk/__data/assets/pdf_file/0021/149124/adults-media-use-and-attitudes-report.pdf

4 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/801429/Education_inspection_framework.pdf

5 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/835733/Keeping_children_safe_in_education_2019.pdf

6 https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/tackling-online-harassment.aspx

7 Davidson et al. (2019). Adult Online Hate, Harassment and Abuse: A Rapid Evidence Assessment https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811450/Adult_Online_Harms_Report_2019.pdf

8 https://www.bbc.co.uk/news/uk-48366835

9 https://www.bbc.co.uk/news/newsbeat-43987148

10 https://www.bbc.co.uk/news/uk-england-cornwall-45735591

digital natives[11] are extremely unhelpful, stereotyping a whole generation who are, in some inexplicable way, digitally aware simply as a result of growing up in an increasingly digital society.

And yet stark digital divides remain across socio-economic, gender and geographic clusters – and there is, in reality, a considerable diversity in young adults' ability to use the internet, their knowledge of it, and their opportunities to access and interact online[12]. There also appears to be a mistaken assumption across the sector that students receive 'online safety' education in schools and, therefore, transition to university equipped to deal with issues of online harassment, abuse and extortion with no further need for awareness-raising or education around critical digital literacies. Moreover, as borne out in recent press coverage[13], institutions are sometimes concerned that, if they publicly address issues of online safeguarding they may raise reputational risks as a "university with an online harassment problem".

As this report (based on two Freedom of Information (FOI) requests[14] with 135 universities in the UK) suggests, it seems that many universities are unaware of, or fail to acknowledge the role of digital technologies and social media in students' everyday lives, and there is a lack of understanding of rights, legislation and social behaviours that can place students at risk of harassment. This lack of understanding places students at further risk in that they can sometimes fail to recognise such behaviours as harmful and do not know how to report, or how they might turn to their institution for support.

The recent survey by Brook[15] revealed that, while 56% of students have been subject to unwanted sexual experiences, only 15% realised they have been sexually harassed. Moreover, a quarter of women (26%) had been sent unwanted sexually explicit messages but only 3% reported it. Research also shows that some groups of students are more vulnerable to online harassment, for example, due to disability, ethnicity, sexuality or religious belief. However, due to their protected characteristics, they are even more unlikely to come forward to disclose abuse. The lack of awareness of the legal and rights issues associated with online harassment increase vulnerability, and compromise their ability to access appropriate support. Often students are frightened to leave their accommodation, attend lectures or communicate with digital technologies for fear of further abuse. These behaviours have serious consequences for mental health, and reports of depression, anxiety and increased isolation are common. In many cases, students have had to move house or even end their studies to escape from the harassment they have received.

There has been much discussion about changing the culture in higher education around student safeguarding and how difficult this is. Perhaps it's time to take a step away from the need for change and instead, we would argue that is important that this culture is challenged and not normalised. What is also important is that HEIs are not bystanders in these situations. So whenever we are aware of this abuse happening on our campuses and beyond, we need to improve the level of proactivity and increase a victim focus that is currently sadly lacking across the sector.

According to UUK (2019: p. 5)[16] online harassment can be defined as, "the use of information and communication technologies by an individual or group to repeatedly cause harm to another person with relatively less power to defend themselves". Yet according to Davidson et al. (2019) there are no universally accepted terms for online harassment in the current research literature. As such, online harassment remains a broad term, which includes many negative experiences online, (e.g. offensive name calling, purposeful embarrassment, physical threats, sustained harassment, stalking and sexual harassment) and thus, due to the lack of definition, online harassment is considered to vary by person and by context (Davidson et al., 2019).

11 Prensky, M. (2001). Digital Natives, Digital Immigrants. In *On the Horizon* (NCB University Press), Vol. 9, No. 5

12 ONS (2019). Exploring the UK's digital divide available from: https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/articles/exploringtheuksdigitaldivide/2019-03-04

13 See https://www.bbc.co.uk/news/uk-48366835

14 See https://www.gov.uk/make-a-freedom-of-information-request

15 Brook (2019). "Sexual Violence and Harassment at Universities"

16 https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/tackling-online-harassment.aspx

The UUK (2019: p. 9) guidelines recommend that:

> *The senior leadership team to involve stakeholders from across the institution in developing, maintaining and reviewing all elements of a whole-institution approach. In addition to senior leaders, stakeholders could include students, students' unions, relevant academics and professional staff.*

Student unions have an important role to play, yet their role should not be independent of the wider university. What works is a holistic response where everybody with responsibility for students across the university works with wider external stakeholders, all engaging with the issues of online safeguarding. It is everyone's responsibility. Course administrators, for example, might be the front line in recognising these issues, as they are often the first people to hear of student concerns via extenuating circumstances (such as lack of attendance or poor performance). Equally, student support and counselling services need to be aware of how to support students experiencing digital harassment and abuse.

However, a holistic approach has to be driven through effective governance. Senior management and boards need to understand their safeguarding responsibilities toward students and staff, and how digital technologies impact on this. Those with strategic roles around curriculum need to understand how this fits into course content and pastoral development. The UUK (2019: p. 9) guidelines state:

> *If not already doing so, universities transfer sponsorship, ownership and accountability for tackling online harassment to the senior leadership team.*
>
> *To support the oversight of safeguarding issues, universities provide regular progress reports on incidents and outcomes of all forms of harassment, including those occurring online, to university courts and governing bodies.*

Yet how many universities have critical digital literacy or online safeguarding as part of the portfolio for a deputy vice chancellor? Who on the board scrutinises this strategy and practice at their institution to ensure effective online safeguarding and demonstrate due diligence? Our research set out to ascertain answers to these questions. There should be clear governance structures that show how strategy transforms into practice and where stakeholders fit and make valuable contributions to a university culture that is aware, and supportive of, the problems students face related to online harassment and abuse.

What is clear from our research and discussions with students is that these issues are here to stay; students are worried about them and feel vulnerable and unsupported. Through challenging the culture around online safeguarding, we can make them feel that we care about their emotional well-being, and know how to help them tackle online abuse if they are unfortunate enough to be subject to it. This shouldn't be something students face in isolation from their university.

Research Approach

In order to determine the state of the HE sector in the UK, we adopted an approach to survey all institutions using Freedom of Information legislation. The Freedom of Information Act 2000[17] in England, Wales and Northern Ireland, and the Freedom of Information Act (Scotland) 2002[18] 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)[19]. Since the acts' introduction, 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 incidents related to online abuse in institutions.

While we embarked on this study with the intention to submit a single information request, initial responses to the first request raised several other questions around the nature of recording, staff training, and working with external agencies that ultimately resulted in a second request being distributed. We present the findings of these two inquiries below.

FOI 1

In June 2019, we sent a FOI request to 135 universities in the UK asking for information in response to the following:

Query	Rationale
1. 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	To determine where the institutions believe their policies cover online abuse and hate speech
2. The name of your university executive team member directly responsible for student safeguarding	To determine whether the institution has anyone in the senior team who has a responsibility for safeguarding
3. The name of your university governing body/board member directly responsible for student safeguarding	To determine whether the institution has anyone on the board with a responsibility for safeguarding
4. Details of how students can report incidents of online abuse (including image-based abuse and online harassment) or hate speech online in your institution	To determine what the institution believes are the routes available to students to report abuse
5. 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	To determine how frequently abuse is reported and whether the institution documents this type of abuse
6. 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	To determine whether the institution has had to deal with issues it considers sufficiently serious to refer to the police, if at all

Table 1 – FOI 1 queries and rationale

17 http://www.legislation.gov.uk/ukpga/2000/36/contents

18 http://www.legislation.gov.uk/asp/2002/13/contents

19 https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

FOI 2

In September 2019, in order to address some of the questions raised by the responses we had received to FOI 1, we sent a follow up FOI request to the same 135 universities in the UK asking for information in response to the following:

Question	Rationale
1.1 Does your university provide any training to staff on online harassment/abuse? 1.2 If so, is this dedicated training, or is it covered in more generic training on harassment and bullying? 1.3 If it is generic training, please outline what it covers specifically about online harassment/abuse? 1.4. If this is specialist training, what aspects of online harassment/abuse are covered?	To determine whether the institution provides training for staff, and if so what the nature of that training is
2.1 If you do provide training, is the training you provide to university staff about online harassment/abuse mandatory for all staff? If not, which of your staff is expected to undertake the training?	To determine whether this training is mandatory
3.1 Does your university provide training to staff investigating student complaints on online harassment/abuse? Is this training mandatory? 3.2 Does your university provide training to staff investigating staff complaints on online harassment/abuse? Is this training mandatory?	To determine whether the institution provides specialist training for those who might be involved in investigations, and whether this is for student and/or staff complaints
4.1 Does your university provide training to any staff on handling disclosures of online sexual abuse? 4.2 Does this training include handling disclosures by both students and staff? 4.3 Does this training include handling disclosures of online child abuse, e.g. the possession/manufacture/distribution of child abuse images, online grooming, or sexual communication with a child? 4.4. Are there any awareness-raising activities for students related to possession of child abuse images?	To determine whether training and awareness of the more serious aspects on online abuse (i.e. sexual abuse/child abuse images/child grooming) and to consider whether students are made aware of some of these issues
5.1. 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? 5.2. How does the university record complaints that involve both online and offline harmful/offensive behaviour (e.g. the in class and online sexual harassment of a student)? Will the online aspect of the adverse behaviour always be recorded?	To determine whether online abuse and hate speech complaints are recorded and categorised specifically, in order that the institution might be able to determine the volume of abuse on campus and more widely among their student body
6.1. 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?	To determine whether the institution might work with specialist services to support students who become victims of online abuse or hate speech

Table 2 – FOI 2 questions and rationale

Findings

Initially, a number of respondents asked us to clarify the terminology we used in the requests. This is a not unusual tactic to extend response time. Nevertheless, it is worthwhile to make clear the specific nature of the terms in the requests prior to presenting findings:

- Image-based abuse: the act of sharing intimate images or videos of someone, either on or offline, without their consent
- Online harassment: repeated online expression via digital devices and platforms (mobile phones, email, social media, messaging platforms) targeted at a particular person that causes the targeted individual substantial emotional distress and/or the fear of harm. This might include, among other things, repeated or persistent calling or messaging, repeated abusive emails and posts on social media, targeting the individual in a threatening manner
- Online hate speech: Any expression posted via digital technology on, for example, social media platforms, messaging apps, discussion forums and email, that attacks a person or a group on the basis of protected attributes defined in the Equalities Act 2010 such as age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation.

Interestingly, we also had one request 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.*

The above request for clarification was received beyond the 20 working days specified for a response to a request in section 10 of the Freedom of Information Act. We were somewhat surprised that it is the belief of this HEI organisation that safeguarding is normally only a matter for those below the age of majority, given that the statutory requirements for adult safeguarding are well established in law in the 2014 Care Act, and the university sector has been guided by the UUK Changing the Culture report published in 2016 (where safeguarding is mentioned eight times).

FOI1 – Policy, Responsibilities and Incidents

In total we received responses from 130 HEIs. We had one outright refusal claiming section 12 of the Freedom of Information Act exemption[20]:

> 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 10, 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 indication that, in this instance, the institution had no formal or centralised reporting and recording mechanisms for online abuse and, as such, were in no place to tackle them. We also received some incomplete responses and another three partial refusals. For example:

> On this occasion it is not possible to provide all of the requested information. In line with your rights under section 1(1)(a) of the Act to be informed whether information is held, we confirm that the university does not hold information relevant to questions 2, 3 and 6 of your request.

20 http://www.legislation.gov.uk/ukpga/2000/36/section/12

Policies

Across the 130 HEIs who responded to our request, there were a total of 21 types of different policies in the student body which were identified as addressing how the institution tackles online abuse (including image-based abuse and online harassment) or hate speech online. The main policy used by universities relates to student discipline/code of conduct or regulations, with over 80 universities stating that this was their main policy. Just over 40 HEIs reported having a specific Bullying and Harassment Policy, while 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 in their IT regulations and Acceptable Use policies. There were inconsistencies in response, with some HEIs sending several and others claiming reliance upon a single policy. In total, we were sent 266 policies from our 130 responding institutions.

Policies used by universities to address online harrassment and hate crime

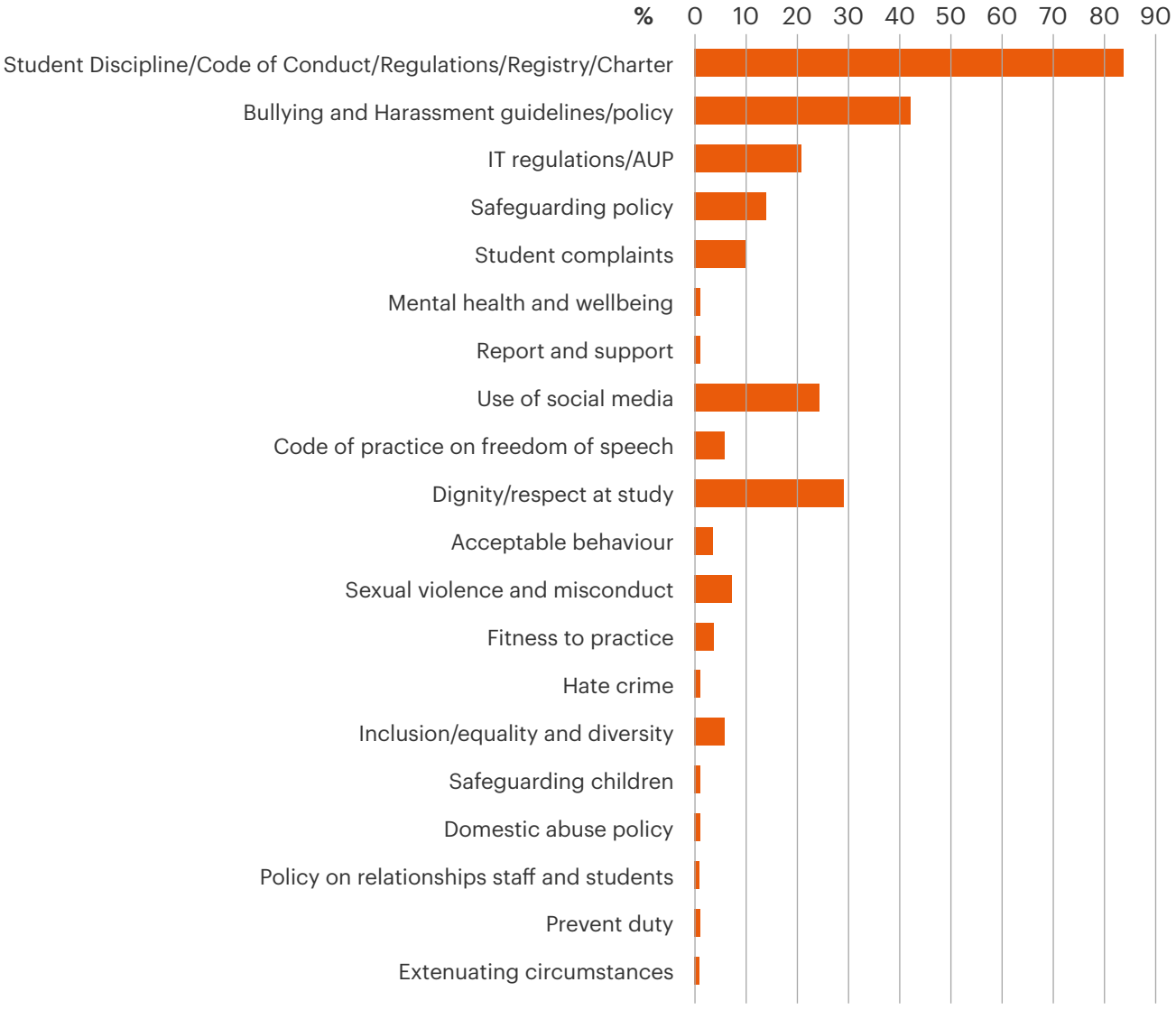


Figure 1 – Types and volume of policies related to online abuse claimed by the UK university sector

We were, in some instances, told that the institution did not need to provide the policy because all of their policies were on their website. However, we reminded those institutions that the nature of the request was to provide us with the policies they believed covered online harassment and hate speech. This is an essential part of the request to understand. Policies provide an organisation with the means on which to base practice in a consistent and organisationally wide manner. Without policy, practice becomes ad hoc and reactive – we wanted to understand where HEIs believed they covered online harassment and hate speech because this would lay the foundation of institutional practice. We received at least one policy from 121 HEIs, suggesting that the other eight did not believe they had policy to cover this (discounting the four refusals).

This makes the analysis of the policies more interesting. Given we would anticipate policies shared by institutions where they have been asked to specifically show they tackle online harassment and hate speech, there are a number of keywords we would expect to see, such as 'online', 'online abuse' or 'hate speech'. We developed a keyword analysis algorithm so we could search the 266 policies, and the results are presented below.

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'

These are all terms one might expect to see in a policy related to online abuse, harassment and hate speech. While pornography is a slight outlier, it was included to see whether institutions were considering the use of this sort of content to harass. Given we received a number of policies from some institutions, we present the results of this analysis in two forms – firstly at a per-policy level, and also combining these policies into institutional sets. In each analysis we considered basic keyword count, as well as proportion of policies that contain the keywords.

By policy

	None	Once	More than once
Online	158	37	70
Social media	143	51	71
Harassment	79	56	130
Online harassment	261	4	0
Online abuse	264	1	0
Hate speech	264	1	0
Hate crime	238	14	13
Digital	232	23	10
Cyberbullying	261	2	2
Cyber bullying	256	6	3
Online bullying	262	3	0
Pornography	254	9	2

Table 3 – Keyword count from policies

At a per-policy level, we can see 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. As can be seen, harassment is well covered but online elements were not. 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, nor 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.

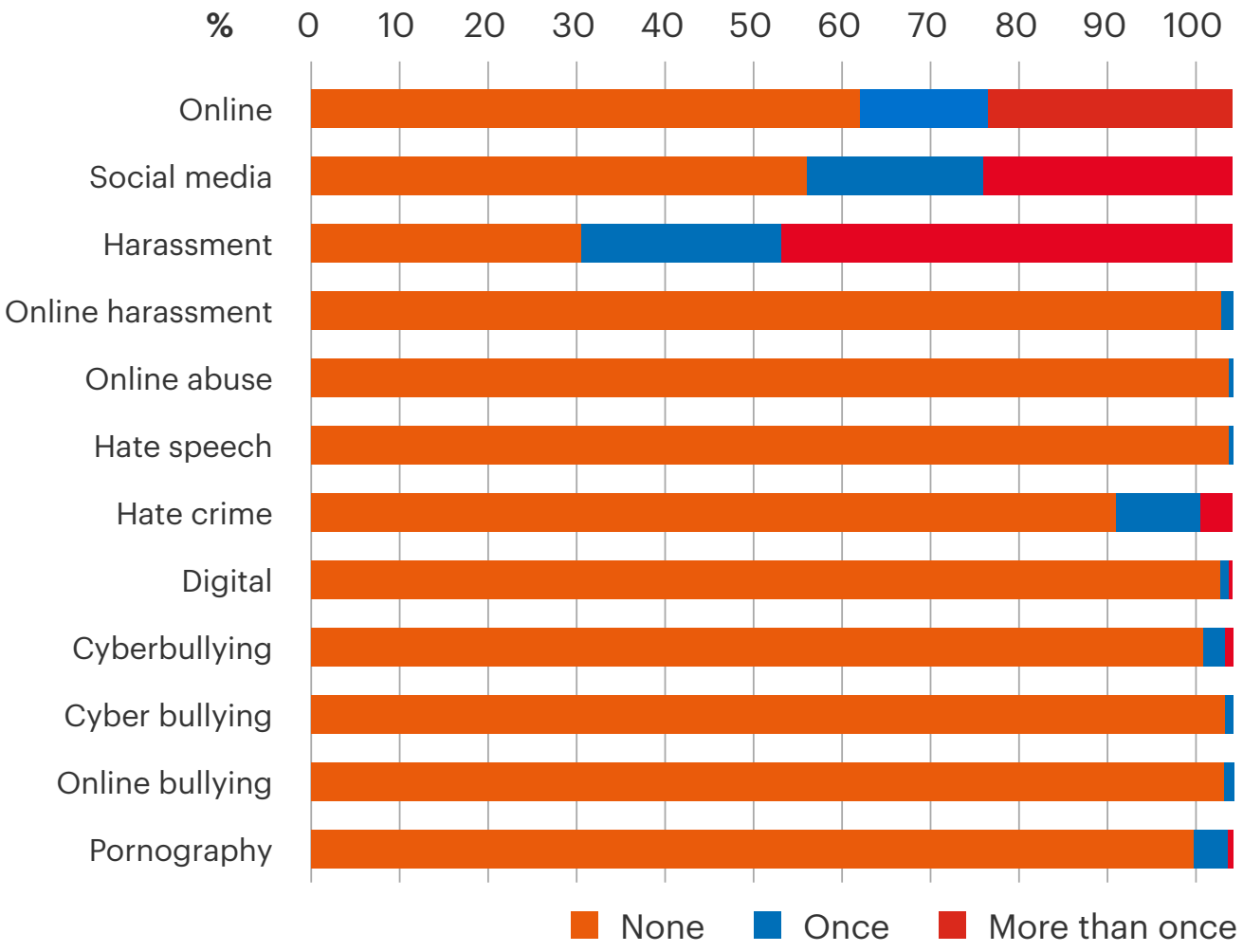


Figure 2 – Proportion of policies containing at least one instance of keyword

By Institution

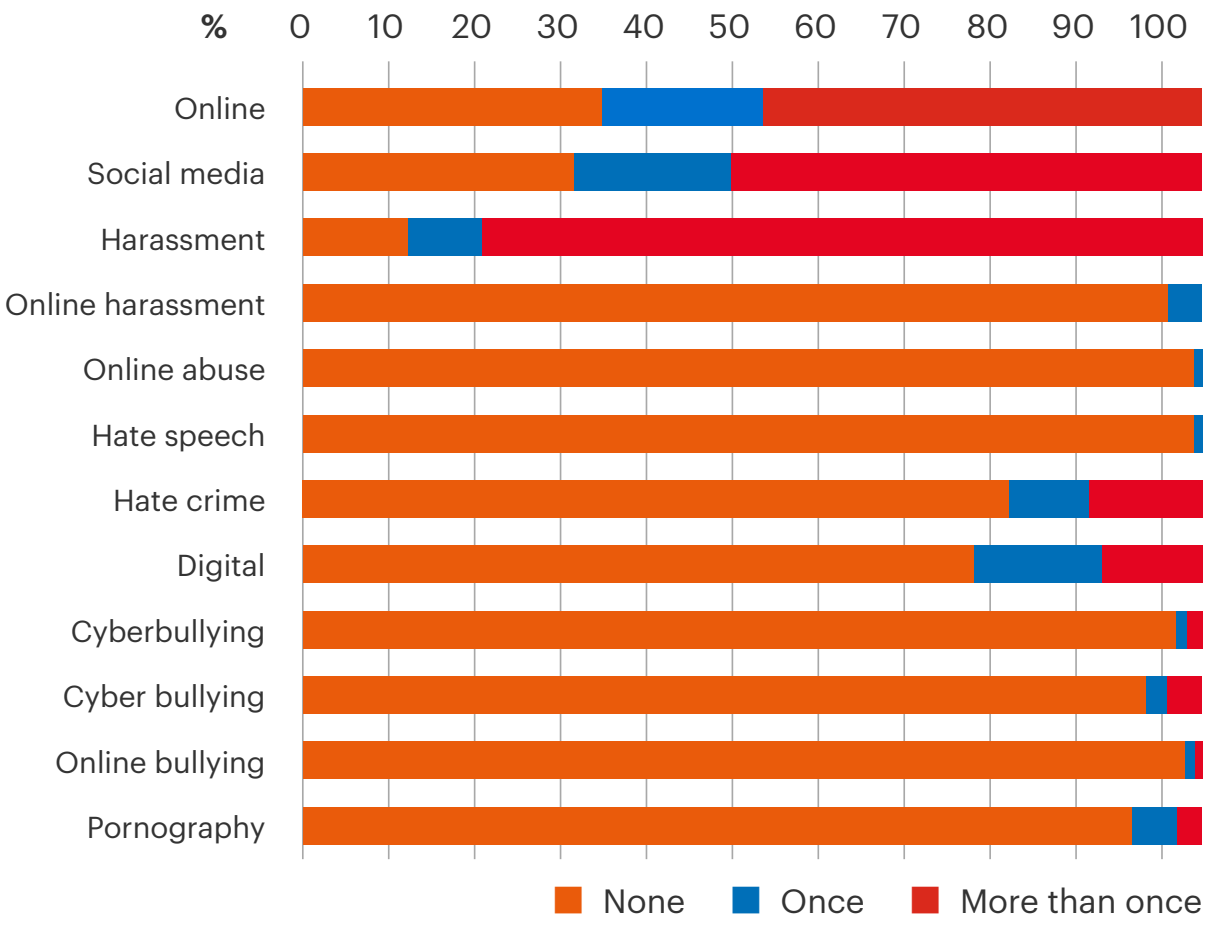
If we combine policies at an institutional level, we see a slightly better picture:

	None	Once	More than Once
Online	40	21	58
Social media	36	21	62
Harassment	14	10	95
Online harassment	115	4	0
Online abuse	118	1	0
Hate speech	118	1	0
Hate crime	94	10	15
Digital	89	17	13
Cyberbullying	116	1	2
Cyber bullying	112	3	4
Online bullying	117	1	1
Pornography	110	6	3

Table 4 – Keyword count from policies aggregated by institution

However, we still see scant coverage of online abuse or harassment with the most 'popular' keywords being 'social media' or 'harassment'. Policy analysis is the foundational aspect of this piece of research because, as discussed above, without policy we can have no confidence that the organisation as a whole has considered these issues or has specified an effective response to these issues. As evidenced by the responses we have received, and the subsequent analysis, the UK Higher Education sector pays scant regard to online harassment and abuse at a policy level.

Figure 3 – Proportion of policies containing at least one instance of keyword, aggregated by institution



Named person for safeguarding on the university executive team

In response to being asked for the name of the member of your university executive team directly responsible for student safeguarding, 110 of the 130 HEIs who replied had a named person responsible, but 15 did not and five refused to respond to the question. Interestingly, a number of replies also stated that as 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.*

On the one hand, we would, legislatively speaking, not disagree with this statement. There is no statutory requirement, at the present time, for HEIs to have safeguarding leads in the same way that schools and colleges educating minors do. There is no comparable document to the Department for Education's Keeping Children Safe in Education document[21] for higher education.

We would, however, (and indeed did in our responses to these HEIs) challenge the view that there has to be a statutory requirement before an institution needs to address student welfare concerns. Indeed, in 2018, the then Higher Education secretary Sam Gyimah[22] wrote a letter to all Vice Chancellors stating:

> *Collectively, we must prioritise the well-being and mental health of our students – there is no negotiation on this. To make this happen, leadership from the top is essential.*

Therefore, it is disappointing to see that some institutions might view safeguarding as something they do not wish to tackle unless there is a statutory requirement to do so. One might suggest that student positive student welfare is good for both the student body and the institution as a whole.

It is, therefore, concerning that there are still a minority of universities where safeguarding is not owned in the senior management team. Moreover, if we consider the number on governing bodies/boards who have visibility over safeguarding, the picture is even more concerning.

Named person for safeguarding on the university governing body/board

Although 109 HEIs reported having a named person on the university executive team directly responsible for student 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, this is concerning. 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.

How students can report

We 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, including the student complaints process; pastoral support systems; student services; student welfare officers, and a range of reporting mechanisms, as illustrated by the response below:

21 Ibid.

22 https://dfemedia.blog.gov.uk/2018/09/16/minister-gyimah-universities-must-ensure-their-mental-health-services-are-fit-for-purpose/

Students can report complaints informally, face-to-face with relevant members of staff; informally via email; formally via the official complaints form. Some third parties may complain on behalf of particular students where we have signed, written permission authorising them to act on their behalf. Where students have disabilities or for other good reasons, the institution will accept complaints via other methods.

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 Universities UK was cautiously optimistic about their use, we would, from a student-centred and organisational risk perspective, suggest that anonymous reporting is a mere sticking plaster that is at best ineffective and at worst highly irresponsible.

If a student reports abuse anonymously, there is little an institution can do to support the student. If the student anonymously reports abuse and names an abuser in the report, is the institution then duty bound to act on the report? And if someone is named, they would then be entitled to see the report as part of a subject access request under section 7 of the Data Protection Act[23], Therefore, 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 large suite of reporting tools.

Given the below responses to the questions about the volume of reporting, we see no difference 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.

Number of student disciplinaries and the number of reports made to the police

	2015/16	2016/17	2017/18	Police (aggregated)
Refused	5.93	5.93	5.93	4.44
Not recorded	14.07	14.07	11.85	32.59
Did not respond	7.41	8.15	7.41	7.41
None	34.07	31.11	25.19	40.00
Less than five	35.56	28.89	37.04	13.33
Between five and nine	2.22	7.41	8.15	0.74
Ten or more	0.00	3.70	3.70	0.74

Table 5 – Incidents reported per year and police referrals (aggregated) reported as percentages

We present data on the volume of recorded incidents and also police referral as a single table. We can see firstly that there is 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 in itself is concerning. In our study, 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 incidents, it should come as no surprise that there are not many recorded disclosures. Given that there are student bodies of several thousand in many institutions, having less than five recorded instances of online abuse in a year seems highly unlikely. This then raises concerns around whether students are reporting this abuse and, if they are reporting it, is it being recorded accurately.

Moreover, referrals to police numbers are so small we have aggregated these figures over the three-year period. We can see high levels where these numbers were not recorded and a high proportion where there were no police referrals.

23 https://ico.org.uk/media/for-organisations/documents/2259722/subject-access-code-of-practice.pdf

Again, it seems unlikely, in a large student community that no incidents occurred that were worthy of police attention. Therefore, we would question whether students were going directly to the police, bypassing the institution completely, or whether universities were just not recording this.

Here again, the universities' responses varied widely. Some stated that they did support students in reporting to the police:

Students access advice and support when they experience/report online abuse, and as part of that we encourage them to report to the police. Some students will report to the police and manage this independently without informing us. We will confirm with the police if we feel there is a risk to the student who has made the report or to the wider university community.

A number of universities stated that they did not record whether incidents were reported to the police, while a number of others stated in their responses to us that reporting to the police was up to the student:

The university does not make reports to the police of cases where online abuse (including image-based abuse and online harassment) or hate speech online was a factor.

Police involvement in these matters would normally be outside the university's control – police may be called but not at the university's request.

We should stress that a high number of recorded incidents would not, in our view, show a problematic institution. We would suggest that in reality this means that an institution has effective reporting and support routes in place, and that students are confident in reporting abuse.

FOI 2 – Training and Recording

The first inquiry resulted in a number of questions being raised, which prompted a second round of questions for institutions. Firstly, we had little confidence of the knowledge base in the sector in dealing with online abuse – as reflected in the diverse nature of policy responses and also the lack of coverage of the issues in policies universities claimed did tackle them. Moreover, we see little challenge at the very top of institutions and reporting/recording data, which would seem very inconsistent with anecdotal discussions around the level of abuse in society as reported by Ofcom[24]. Therefore, in order to try to gain more clarity and understand the problems the sector faced in more detail, the second round of enquiry specifically focused on the nature of training in institutions and also the nature of recording.

Training Provision and Nature of Training

For the second Freedom of Information request, we received 106 responses in total. 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, we cannot hold any confidence that an institution is capable of supporting students who become victims of online abuse when they have neither a documented response nor knowledgeable staff to support them. Online abuse and harassment can be complex both socially and legally – there are no easy answers when supporting those victims of abuse. We know from our work in the school sector[25] that victims will sometimes not recognise their treatment as abuse or harassment and we therefore need staff in the sector that understand the issues, the legal thresholds, and how to support these victims.

24 https://www.ofcom.org.uk/__data/assets/pdf_file/0021/149124/adults-media-use-and-attitudes-report.pdf

25 https://www.mariecollinsfoundation.org.uk/assets/news_entry_featured_image/MCF-Peer-on-peer-Abuse-Research-Report-sunday-final-version.pdf

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. The types of training 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. The two institutions that provided specialist training did, unsurprisingly, cover these details in more depth, with one HEI making use of research expertise in the area (Bedfordshire National Centre for Cyberstalking Research[26]). However, any training that attempts to look at issues related specifically to online abuse is few and far between. 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 staff on any aspect of online abuse or harassment.

Investigators Training

As part of the exploration around training provision in HEIs, we also asked if investigators or others who might be involved in student and staff complaints, and student support, received specialist training about online harassment and abuse. We might hope that this would be the case, because these are the people dealing with complaints being made so might need a deeper understanding of the issues associated with online harassment so they might execute their duties correctly. We asked the question for both student and staff complaints. In the case of student complaints, 60% of respondents said that they did no training, while for staff complaints that figure was slightly higher – 62%. Two HEIs responded to say that the question related to student complaints was not applicable to their institution, and three said similar about staff complaints. In one case, this was because the respondent stated their main investigator was a former police officer so did not need further training. Such confidence may be misplaced as we consider how quickly both law and practice evolve in this field. For example, there was no legislation specific to image-based abuse until 2015, and nothing related to upskirting until 2019.

Of those who did provide training (38% for student complaints, 35% for staff complaints) the majority of respondents said they provided training for investigators, with an even smaller set of respondents saying (6% for student complaints, 9% for staff complaints) that 'other' staff also received training. These 'other' staff were generally front-line staff, such as student services, who might initially deal with an upset student. This is the level of staffing we might expect to see receive this sort of training, but it appears to only happen in a very small subset of our respondents.

26 https://www.beds.ac.uk/irac/centres/nccr

Online Sexual Abuse Training and Awareness Raising

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. Again, we know these are issues that university students have faced (such as an attempt to sell images and videos of an ex-partner online[27]) and sometimes have complex elements (for example, the image-based abuse case reported from a University of Lincoln student who had used images of an ex-boyfriend in an exam assessment where she was ultimately acquitted[28]). 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 Well-being 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.

We also considered the coverage of training around child abuse images, grooming and sexual communication with a child (being aware that cases of students engaging in such illegal activity do exist [29] [30]), which we discovered was rarely covered in this training (only 13% of respondents).

Finally, we asked whether students received any awareness training around possession of indecent images of children. The Home Office, alongside the Internet Watch Foundation, Marie Collins Foundation and NSPCC, have produced the Steering Clear campaign[31] and we were aware, as a result of our work on this project, that one of the target audiences for these resources was university students. However, this campaign was not mentioned at all in any responses and only one institution said they had delivered any such awareness-raising to students. We would suggest that this is a concern because, while cases such as the one referenced make the headlines, we are aware, as a result of our own work with students, that some might arrive at university with images of peers from school. While they might have a view that because these are images of peers, they do not fall under the legislation for the possession, manufacture or distribution of indecent images of a minor, they very much do, and once past age of majority (i.e. when they start at university) these possessions would be taken very seriously by law enforcement and could result in a custodial sentence for a sexual crime.

Three institutions that did no awareness-raising around possession of indecent images of children stated that this was covered at a policy level, because possession would breach Acceptable Usage and IT policy. We are sure that this would not actually be the case if the images were on a student's personal device rather than university storage. It would seem to extend the reach of the policy beyond what would be reasonable due diligence, unless they are claiming that universities are responsible for content on personal devices that use their networks. We might suggest this would be a highly dangerous thing for a university to do! However, it did demonstrate that the view of the universities was not to support students, but to protect the institution in the event that a student might be found in possession.

Finally, one respondent said their institution would be starting awareness-raising 'soon'.

27 https://www.bournemouthecho.co.uk/news/17779324.revenge-porn-student-spared-prison/

28 https://www.telegraph.co.uk/news/2018/04/12/art-student-charged-wth-revenge-porn-submitting-photograph-topless/

29 https://nouse.co.uk/2019/07/26/former-student-receives-prison-sentence-following-sexual-communication-with-children-

30 https://www.gazettelive.co.uk/news/teesside-news/student-amassed-collection-grotesque-images-15939356

31 https://stoponlinechildsexualabuse.campaign.gov.uk/

Recording Incidents

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 categorise 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 categorise (60% for online abuse, 77% for complex complaints) these reports, and around 15% saying they would record as both online and the more general categorisation (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 categorise incidents stated somewhat confusingly that categorisation was not needed because they used anonymous reporting. What was clear from the myriad of responses, however, was that it is unlikely institutions accurately categorise 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 categorisation, two respondents referring to the Office of the Independent Adjudicator for Higher Education guidance on good practice for handling student complaints and academic appeals[32]. This guidance provides no indication of how one might categorise incidents, so it seems strange to refer to it in a question on categorisation. However, it does go into some detail around using recording as a mean of understanding the nature of complaints to inform training and process improvement:

> *28 Concerns, complaints and academic appeals should be recorded in sufficient, proportionate, detail....*
>
> *29 When information is recorded and used in this way, it helps providers to identify and address the causes of complaints and academic appeals. Providers may identify training opportunities and, where appropriate, improvements can be introduced.*

Again, without effective categorisation of incident, we are unsure how a university might better understand opportunities for improvement or training.

Working with External Bodies

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 aware from the Office for Students Catalyst projects[33] that there was a tendency to provide support in house rather than utilising established external services in some cases 'reinventing the wheel' related to things like support helplines. We were, therefore, unsurprised to discover that the vast majority (73%) of respondents stated that they 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.

32 https://www.oiahe.org.uk/media/1859/oia-good-practice-framework.pdf

33 https://www.officeforstudents.org.uk/media/e3c0bd5e-7e03-4235-941a-f933da269728/catalyst-evaluation-summative-report.pdf

Key Findings

What is clear from our findings is this is not a sector that has established policy or practice to support students who might become victims of online abuse and harassment. We see pockets of good practice, but we also see the majority of institutions who have little by way of policy, practice, recording or training that is anywhere near an effective response. What focus there is lies on the protection of the institution, rather than the support of students.

This starts at the policy level and continues into practice. As we have stated above, without the foundation afforded by effective policy, we have no expectation that an institution is sufficiently aware of the issues their students face or have any means to tackle them in a uniform manner. We have seen in our responses a vast range of policies being proposed as the location from which online abuse is addressed. Yet in analysis of these 266 policies, we see the majority having little awareness whatsoever of online issues. In the majority, those policies universities have reported to us as tackling online abuse and harassment pay lip service at best. While there are a few examples of good practice these are few and far between.

We see safeguarding being considered a senior management responsibility in the majority of institutions yet we still received responses from 20 that did not. While it is encouraging to see a high number of institutions having someone on their senior leadership team with responsibility, it is far less promising to see only 43 having someone on the board who might provide scrutiny to the senior team on their performance.

We saw very low levels of recorded incident of online abuse in universities, which would either suggest that universities are oases of virtue in a world where online abuse is common, or that other factors meant that either students were not reporting abuse to institutions or these reports were not being effectively recorded. We are sure, from what was reported to us and responses related to how incidents are categorised, the latter is the case. We also saw a reliance on anonymous reporting in a number of cases, viewed by some institutions as a positive tool to allow students to disclose abuse. However, it would seem, given the volumes of reporting, that this was not necessarily used effectively, and moreover, anonymous systems provide little opportunity to actually support a victim of abuse or bring an offender to justice.

We also saw a highly concerning lack of training around online abuse, with few universities providing specialist training. Those who did claim to cover it, on the whole, would address it as a facet of things like bullying, harassment or equality and diversity. We have highlighted in this report the differing nature of online abuse and how it is necessary to have differentiated training in order to recognise abuse when it occurs and how an institution might best support students. However, from our investigations we see training is at best patchy and inconsistent. There is certainly no national coordination around online abuse training in universities. We also see a failure to relate online technologies to more serious sexual abuse, harassment or criminal activities related to minors, even though we know these sorts of abuses occur in university settings. Moreover, we see an almost sector wide failure to raise awareness among students of the dangers in possessing indecent images of minors, as well as concerning arguments that a breach of policy is sufficient to tackle these issues.

Clearly, we would like to see the university sector take their duty of care responsibilities seriously related to supporting students who are the victims of online abuse, and we would rather the sector responded because they believe student welfare, effective reporting and consistent staff training are all good things to do, rather than things they will resist until statutory duties are imposed. There is a long way to go. What we see from the results of our inquiries is not even a ‘postcode lottery’ – in a lot of cases, how a student who is a victim of online abuse, harassment or hate speech is treated by their university is not just down to where they are, but also to whom they are speaking.

Recommendations

Universities should:

- Have effective, specific policies related to online abuse and hate speech, rather than tacked on to others
- Have at least one named senior leadership team member with a responsibility for safeguarding
- Have at least one named board member with a responsibility for safeguarding who can scrutinise the strategic direction in the institution
- Use reporting mechanisms that students are confident in using, that result in them being listened to. Transparency reporting of recorded incidents can be used to show students and the wider stakeholder group that reports are taken seriously and acted upon
- Have staff training specific to online abuse and harassment for all staff who might support student welfare
- Ensure that there is effective recording of complaints and incidents so the institution can understand the nature and volume of problems and inform strategy accordingly
- Work with external agencies where appropriate, to provide additional lines of support for students and to build institutional knowledge related to online abuse and harassment
- Make use of the Online Safeguarding Toolkit[34] to self-review organisational policy and practice and build an action plan to improve.

34 https://www.uos.ac.uk/sites/default/files/Higher-Education-Online-Safeguarding-Self-Review-Tool%202019.pdf

University of Suffolk

Published by University of Suffolk

978191316008 Digital (download only)