



Professionals Online Safety Helpline Analysis 2021-2022

Exploring the Issues Professionals Face in Supporting Young People with Staying Safe Online

Prof Andy Phippen, February 2023

Executive Summary

As part of the UK Safer Internet Centre, the Professionals Online Safety Helpline¹ (POSH) is operated by SWGfL. It has been running for over 10 years and in this time it has handled over 24,000 contacts and more than 11,000 online safeguarding issues.

The analysis in this report is drawn from a total of 4,078 cases recorded by the helpline between 1st November 2021 and 1st November 2022, and is compared to a previous analysis that explored the COVID lockdown period 2020–21. It conducts a measurement of the types of calls; where they come from, and who made the enquiries. Also included is a top level qualitative analysis of the nature of these calls that fall within categorisations as defined by the helpline.

KEY FINDINGS ARE:

1

There has been a significant increase in enquiries to the helpline. However, a breakdown of these calls, and their source, revealed little evidence of serious online harms being the reason for these cases.

2

Most concerns are from school settings – particularly secondary schools.

3

The vast majority of enquiries relate to social media content that has the potential to negatively impact a school's reputation and professional standing. An example of this is content that show pupils criticising staff and potentially making defamatory comments.

4

Because there is no national coordination on the issues, schools don't know how to respond or understand thresholds for determining the severity of response. Therefore schools, potentially without specialist training, have to make decisions on their own.

5

A lot of enquiries may express a concern about a specific post or piece of content. But more of these broadly highlight that professionals wish to be better informed around media literacy. Most encouragingly, they are contacting the helpline because they don't feel that they have the capacity to deal with online safeguarding issues on their own.

6

A quick enquiry to the helpline often improves their understanding, or clarifies whether there is a need to escalate concern.

7

Professionals calling the helpline are not always aware of tools available on the major platforms to block and report themselves. Clearly, there is a need for training and the sort of information provided in the Online Safety Live sessions that SWGfL² provides free of charge.

8

The helpline analysis highlights frustrations professionals have in dealing with social media platforms for support, take downs, etc. and the importance of platform liability that's being tackled in the Online Safety Bill.

9

However, a lot of the harms disclosed to the helpline would not be in the scope of the bill. It's also important to support multiple stakeholders in the online safety space, rather than assuming increased platform liability will eliminate online harms.

Introduction

The Professionals Online Safety Helpline³ is a free service for professionals and volunteers working with children and young people. It provides signposting, advice and mediation to resolve online safety issues staff face about themselves. These might be around protecting professional identity and online harassment, or problems affecting young people, such as cyber-bullying or sexting. The below quote illustrates the type of enquiries helpline practitioners deal with on a daily basis.

The helpline is open Monday to Friday, during normal working hours, and aims to respond to calls within three hours where possible. The main benefit of using the helpline is the exceptional contact it has with industry partners, which enables the reporting of issues to a real person. It also helps industry keep helpline practitioners up to date with policy and reporting changes.

The helpline has been in operation for 10 years, in this time the helpline has handled over 24,000 contacts and helped with over 11,000 online safeguarding issues. As part of the UK Safer Internet Centre, the helpline is operated by SWGfL.

"To Whom It May Concern

It was reported to myself and the Principal earlier today that derogatory comments and video clips about several members of staff have been uploaded onto TikTok. The video clips are a defamation of their character and completely false.

The defamatory clips have been deleted but we would appreciate if you could support us with this matter and report to TikTok. Your support may ensure swifter action might be taken by TikTok. Our staff members are extremely distressed and this has caused great upset.

We have reported our concerns to TikTok and to the police."

ANALYSIS

The analysis of the helpline in 2022 is drawn from the cases recorded over that period. It conducts a measurement of the types of calls, where they are from, and who made the enquiries. There is also a high-level qualitative analysis of their nature within categorisations as defined by the helpline. The analysis is based upon 4,078 cases taken between 1st November 2021 and 1st November 2022. This shows a significant increase in the use of the service compared to the previous analysis from 2020–21 which considered 518 cases between 16th January 2020 and 23rd January 2021.

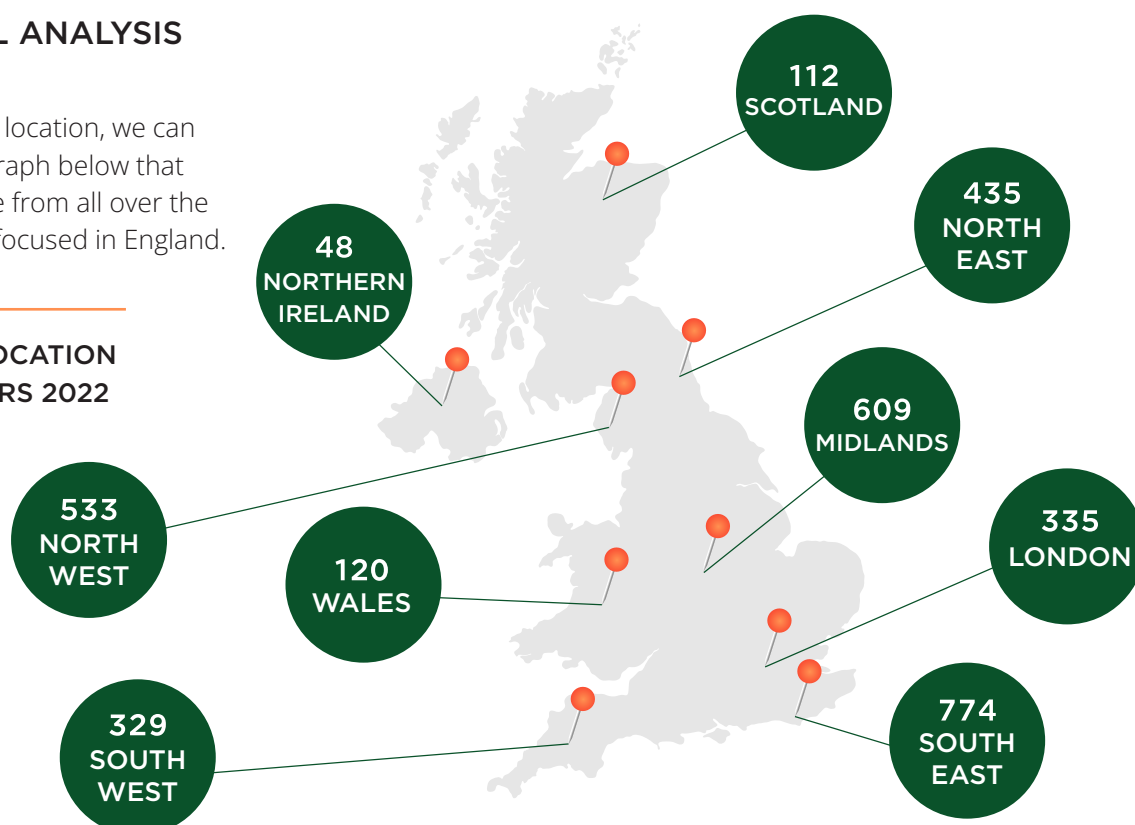
The case recording system details the full dialogue of each enquiry – the majority of these being supported through online communication via the Professionals Online Safety Helpline email. However, a minority of cases were also supported over the phone with the discussion recorded by the practitioner. The system also recorded, in most cases, the location, and the enquirer can categorise the enquiry, which the practitioner can add to. Further detailed analysis of the cases, using illustrative examples, demonstrates the breadth of the enquiries received by the helpline – allowing for a detailed lens onto the online safeguarding issues faced by professionals in the UK.

This analysis considers, in the first instance, POSH cases across the 12 months between November 2021 and November 2022, including changes in the nature of enquiries from the previous analysis. It also includes a top-level comparison between enquiries from primary and secondary school settings. However, as can be seen in that section of the report, the difference in volumes between the types of setting means that it isn't possible to directly compare.

TOP-LEVEL ANALYSIS

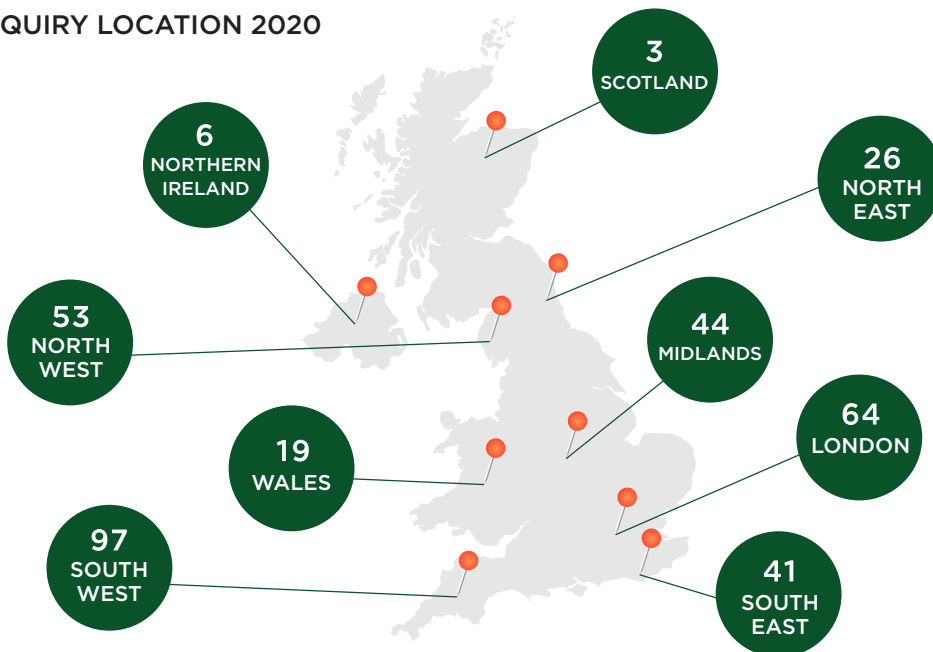
In terms of the location, we can see from the graph below that enquiries came from all over the UK, with most focused in England.

FIGURE 1 - LOCATION OF ENQUIRERS 2022



While there's not much to infer from the location of calls, this is worthy of note because it shows the national reach of the helpline. Compared to the 2020 analysis, shown in figure 2, the spread is now far more diverse. The South West, once the most common region for enquiries, is now one of those receiving the fewest.

FIGURE 2 - ENQUIRY LOCATION 2020



Enquirers will generally make use of electronic communication (i.e. email) to contact the service, with 4,019 enquiries taking this route. The service also deals with a small number of phone calls (59), where practitioners record the nature of the enquiry, during and after the call.

The helpline is promoted as a service for professionals dealing with online safety issues. We can see in Table 1 that the vast majority of enquiries are drawn from enquirers who work with children. While most, as we would expect, are teachers in schools, others represent a wider range of professions. There are also a handful of parents who have made use of the service. In the case of 'Other/not specified', there have been direct enquiries from young people who have disclosed being at risk or harmed. While the helpline supports these cases where they can, in some instances, they will signpost child-specific services such as the NSPCC.

TABLE 1 - TYPE OF ENQUIRER

2022		2020
3	CHARITY/NGO	0
63	GENERAL PUBLIC	51
33	LOCAL AUTHORITY	6
9	OTHER PROFESSIONAL	73
187	OTHER SCHOOL STAFF	2
19	PARENT	15
28	POLICE	28
7	SOCIAL WORKER	35
3,461	TEACHER	276
210	OTHER/NOT SPECIFIED	32

TABLE 3 - NATURE OF ENQUIRIES RECEIVED BY THE HELPLINE

2022%	2022 VOLUME		2020 VOLUME	2020%
81.780284	3,335	SOCIAL NETWORKS	227	43.82239
75.870525	3,094	ONLINE REPUTATION	148	28.57143
9.8087298	400	CYBER BULLYING	67	12.93436
1.814615	74	POTENTIALLY HARMFUL CONTENT	21	4.054054
1.0789603	44	WEBSITES	42	8.108108
0.6130456	25	TECHNICAL SETTINGS	17	3.281853
0.416871	17	REPEATED HARASSMENT		0
0.3678274	15	SEXTING	12	2.316602
0.3187837	13	MEDIA LITERACY EDUCATION	99	19.11197
0.3187837	13	SEXUAL HARASSMENT	14	2.702703
0.3187837	13	DATA PRIVACY	12	2.316602
0.2697401	11	LOVE, RELATIONSHIPS AND SEXUALITY	3	0.579151
0.2452182	10	E-CRIME	8	1.544402
0.2206964	9	APPS	21	4.054054
0.2206964	9	GROOMING	16	3.088803
0.2206964	9	PEER-ON-PEER ABUSE	16	3.088803
0.1716528	7	MOBILE DEVICE	11	2.123552
0.1716528	7	SEXTORTION		0
0.1226091	5	HATE SPEECH/RACISM	5	0.965251
0.0980873	4	EXCESSIVE USE		0
0.0245218	1	GENERAL ENQUIRY		0
0.0245218	1	GAMING		0
	4,078	TOTAL ENQUIRIES	518	

It can be seen from the table above that a lot of enquiries related to low-level concerns. And issues of a potentially criminal nature (e.g. harassment, sexting, e-crime and hate speech) are very much in the minority. However, there are certainly some within reputation and social media categories that could potentially have civil implications (e.g. defamation).

The 2020 comparison also allows us to consider how the nature of the service has changed. While in 2020 the service was dealing with online reputation concerns in 28% of enquiries, this has increased significantly to 75%. In the vast majority of cases, the helpline is now supporting schools who have experienced challenges with social media posts related to content that might negatively impact on the school. Some of this might be considered a low-level concern compared to those enquiries tackling challenges that are more criminal. But, the sample of cases included in Appendix A illustrates the severity of some of the content, which could potentially be defamatory in nature.

Appendix A contains an anonymised sample of enquiries where the helpline has dealt with at least 10 different categories. While not an exhaustive analysis, it does illustrate the range of cases that are dealt with by the helpline and the nature of the

discourse associated with them. For example, even if some cases might be considered less severe, the concerns and impacts upon school staff are highlighted.

When considering other changes between 2020 and 2022, in terms of the percentage of enquiries, there's a significant drop in those related to media literacy. In the past, almost 20% of enquiries related to how to tackle online harms issues in the classroom and broader education questions around online safety. These have fallen to less than 1% of enquiries now. In other cases, such as cyber-bullying, these remain at around 10% of enquiries. And while some of the more serious categories, such as harmful content, sexting and harassment, do not count for significant numbers of enquiries, the nature of these in Appendix A shows that, in some cases, schools are dealing with serious criminal issues.

DIFFERENCES BETWEEN PRIMARY AND SECONDARY SETTINGS

Enquirers are invited to include the type of setting in which they work. While a proportion of calls come from outside of education, using this data does allow us look at the differences. In total, 109 cases were tagged as primary settings and 3,401 as secondary. This very clearly shows that the service is used far more by secondary settings. The table below shows the nature of the enquiries:

TABLE 4- COMPARING THE NATURE OF PRIMARY AND SECONDARY ENQUIRIES

	SECONDARY VOLUME	SECONDARY %	PRIMARY VOLUME	PRIMARY %
SOCIAL NETWORKS	3,147	92.53161	72	66.05505
ONLINE REPUTATION	2,945	86.59218	66	60.55046
POTENTIALLY HARMFUL CONTENT	347	10.20288	15	13.76147
CYBER BULLYING	28	0.823287	9	8.256881
WEBSITES	17	0.499853	8	7.33945
PEER-TO-PEER ABUSE	9	0.264628	3	2.752294
TECHNICAL SETTINGS	9	0.264628	2	1.834862
SEXTING	8	0.235225	2	1.834862
MOBILE DEVICE	6	0.176419	1	0.917431
DATA PRIVACY	5	0.147016	1	0.917431
GROOMING	5	0.147016	1	0.917431
SEXUAL HARASSMENT	5	0.147016	1	0.917431
APPS	4	0.117612	4	3.669725
E-CRIME	4	0.117612	0	0
LOVE, RELATIONSHIPS AND SEXUALITY	3	0.088209	1	0.917431
MEDIA LITERACY EDUCATION	3	0.088209	1	0.917431
EXCESSIVE USE	2	0.058806	1	0.917431
HATE SPEECH/RACISM	1	0.029403	1	0.917431

While the difference in volume of calls makes it difficult to directly compare, the data can indicate the nature of the relationship different settings have with the helpline. Clearly the helpline is more widely used in secondary settings, and in the majority of cases this will help with issues affecting reputation or abuse of staff. However, in 10% of cases callers are asking about potentially harmful content. Primary schools still contact about reputation and social media in the majority of cases, but higher proportions of calls relate to cyber-bullying and concerns about specific websites. And in the more severe, but minority of calls, secondary settings are more likely to be faced with criminal activity.

“ In 10% of cases callers are asking about potentially harmful content. ”

IMPLICATIONS AND EMERGING ISSUES

The above analysis highlights a number of key findings. Firstly, the helpline provides an essential service that has supported over 4,000 online safety concerns throughout 2022. Secondly, as with the 2020 analysis, the power of the data from the helpline is that it allows exploration of what's happening at the grassroots level in education settings and within the children's workforce. This is something which perhaps highlights a less severe picture than the media might represent.

While the data clearly shows, as illustrated, that some settings are dealing with extremely serious cases, some of a criminal nature, these are very much in the minority. Schools are not contacting the helpline to ask for support in dealing with extreme cases on a daily basis. However, it is important to stress that only the data presented can be analysed – and it's the more extreme issues that professionals are asking for third-party support with. It cannot be concluded that because the helpline is not receiving high volumes of calls, these issues are not occurring. However, if the data is compared with analyses from other helplines operated by SWGfL (such as the Reporting Harmful Content service), it can be seen that 'low-level' concerns are the day-to-day reality for professionals working with children.

Clearly the most significant number of enquiries relate to issues of reputational damage and content posted by students (and further afield) that criticises institutions and staff. And with some severe cases, there's the potential for defamation. This is a complex issue – and at the present time – we don't have any national guidance. At one level, it's suggested that the best thing to do in a lot of cases where the content is not receiving many views and shares, is to ignore what will soon disappear in the mass posting of new online content. And, in some cases, it's suggested that reacting excessively to these cases, and referring to them as 'defamation' in a playground setting, will actually encourage further posting.

However, there are some cases where content could be considered defamatory or grossly offensive, and could potentially meet the criminal threshold. While it is unlikely that, due to the age of those posting content and public interest, such concerns would result in a police and criminal justice response, they do need to be tackled and staff who have been abused should be supported. As there is currently no national guidance on these issues, schools rely upon services, such as the helpline, to tackle these issues.

Certainly the helpline will generally have more success in removing content from major platforms in the event that the helpline has investigated and concluded that the content does breach standards on the platforms on which it's been posted.

Consistency is important in terms of policy development and response to these instances. There's a need for guidance on thresholds for concern, and up-skilling the workforce so they can use the tools provided by platforms better so they can tackle these issues in a consistent manner.

Currently, a school has no clear guidance on whether they should take a 'humorous' piece of content posted by a pupil viewed a few times seriously, and how the response to this should be different to content that threatens or defames. The helpline has a role to play in this, but for the enquiries that are very much: "I do not know how to deal with this," in nature, we would hope that some national guidance would help professionals be more consistently supported.



The helpline provides an essential service that has supported over 4,000 online safety concerns throughout 2022.

“

It is clear from the cases recorded by the helpline that many professionals will seek support.

More broadly, a common theme running through the enquiries is a reaction around a safeguarding alert, a media rumour, or simply not knowing what to do in a given situation. This again highlights the need for digital literacy development by the children's workforce. It is clear from the cases recorded by the helpline that many professionals will seek support

rather than trying to resolve an issue in isolation. Here, a quick enquiry to the helpline often improves their understanding or clarifies whether there is a need to escalate concern.

RELATING TO THE PRESENT POLICY CONTEXT

From reflecting on the findings in the analysis to looking at the wider online safeguarding landscape, at the time of writing this report, a key issue is discussion and debate around the Online Safety Bill⁵. Within the draft bill is legislation aimed at ensuring platforms conduct risk assessments on safety features offered with their services. There is also a requirement to show duty of care in supporting their users to be safe. While this report is not the place for a detailed legal examination of the issues in the bill, the casebook from the helpline does demonstrate the considerable frustration felt by professionals when reporting content and asking platforms to remove it. Alongside this while it is rare in case descriptions to know exactly the processes enquirers have gone through, it's not unusual for them to state to the helpline that they have contacted the platform who are remaining silent.

Certainly, expectations in the bill to encourage platforms to be more transparent with their reporting routes, and to take down harmful content, is to be welcomed. However, it can be suggested that the data from the helpline helps highlight that the bill is not the solution to tackling online harms.

Legal but harmful provisions have now been removed from the bill, which is unsurprising given the legal and rights-based challenges in subjective harms and how platforms might address them. However, a lot of enquiries to the helpline would fit into the category of potentially legal but harmful. It also emphasises the importance of platforms being responsive to disclosures, and the need to up-skill the workforce, to help professionals develop their knowledge on using these online safety tools, while also understanding the thresholds and the magnitude of online harms. As such, we anticipate a little reduction in the use of the helpline following the bill.

“

It also emphasises both the importance of platforms being responsive to disclosures, and the need to up-skill the workforce.

Conclusions

This analysis of the Professionals Online Safety Helpline's case records demonstrates the breadth of issues professionals face regarding online safeguarding. Pointing a lens into online safeguarding practice among professionals highlights the low-level nature of a lot of the issues they deal with, as well as the seriousness of some incidents. What is clear are concerns around online defamation and content that challenges the reputation of schools. This has increased significantly in the last two years, and is by far the most common reason for a professional to contact the helpline. It has certainly been a great success in supporting them and removing offensive content that breaches community standards. However, in a lot of cases, expectations management is a key part of what the helpline does.

Furthermore, evidence from the helpline once again shows that online safeguarding is a team effort and we cannot expect a single stakeholder to have all of the solutions. It is far better for a professional to reach out to partners, such as the helpline, to support them with an online safeguarding issue, rather than feeling like they have to resolve it on their own.

As with other helplines operated by SWGfL, POSH has good relationships with all major social media providers, and with police, social care and other support services, such as the NSPCC and CEOP. Once again, the analysis shows that the nature of online safeguarding is diverse, complex and covers a broad range of issues. Professionals need support and national guidance on how to tackle defamatory content relating to schools and the people that work in them.



APPENDIX A – SAMPLE ENQUIRIES FROM CATEGORIES WITH TEN OR MORE CALLS

Please note that the following examples are indicative of the nature of the enquiries received, they are not an exhaustive list. They are included in this report to highlight the breadth of enquiries staff at the helpline have to deal with, and also the issues related to online harms that schools have to tackle on a daily basis.

SOCIAL NETWORKS

Enquiries related to problems with social media platforms, for example: fake accounts, abusive posts or problematic comments related to schools and staff, and take downs associated with these platforms.

An account has been set up on TikTok and shared to Instagram with a photoshop of my head on strippers bodies saying I am not a slag I'm a real slag with various hashtags. The accounts are @`{username}` and @`{username}`. I have reported the videos to TikTok but have been unable to do the Instagram account as I cannot see the account name. I have reported harmful content and I have also made a 101 police report of it.

What else can I do to get this taken down and for the info who created these accounts to be shared with the police?

I am a Network Technician at `{school}`, and I was wondering if you could give us some advice regarding TikTok accounts. There have been some TikTok accounts created dedicated to harassing members of staff which have quickly spread through the school and come to the attention of SLT and other staff within school. We have reported the accounts and videos to TikTok, but we don't believe that this `{{name}}` be enough, and we can't find a way of contacting TikTok directly to discuss this. It appears to have become a big problem within schools this week and I have been directed to your organisation for some help. Any help would be greatly appreciated!

We have a growing concern in our school and community at the amount around a Instagram account that has been created called `{username}`. The opening comment on this page says "post s**t about people anonymously" and then there is a link to `{url}`.

We do believe that this could have been created by a student in the school but we can't confirm this. We are greatly concerned about the nature of a lot of the comments on this account, some of which are causing real upset to our students and parents (please see attached screenshots).

SOCIAL NETWORKS

(Continued)

We are requesting as much support as possible from Instagram and {{username}} in being able to close down this account or even find out who has created it. It seems appropriate that we are also asking for this help on Safer Internet day.

Please could someone get back to me as a matter of urgency due to the number of parents that are expecting action.

We have an angry parent who is making slanderous comments about staff in the school via Twitter. Is there a way you can support us via the professional helpline to have these removed?

ONLINE REPUTATION

Posts making claims against the professional conduct of schools and staff.

We have been made aware of some TikTok accounts which have been setup using our Academy logo which contain videos of our staff with nasty and derogatory comments.

The usernames we have been made aware of are: @{{username}}, @{{username}} and @{{username}}

Is this something you would be able to support us with at all please?

Please can I report a number of Tik Tok accounts to you for closure. These videos are defamation of character and therefore impacting on the well-being of staff within our academy.

Please can I request the following accounts are closed off the social media platform TikTok

{username}

{username}

{username}

Please can you update me with the requests.

If you require any further information, please do not hesitate to contact.

ONLINE REPUTATION

(Continued)

I am hoping that you can help me.

We are having some real issues with spoof accounts (TikTok and Twitter in particular) using the school identifiers (badge etc.) and the images of staff to create content that is highly offensive and damaging. Despite our own efforts and reporting the material on numerous occasions we are no further with resolving the issues (TikTok in particular). We have reported this to the local police, who seem unable to help.

As seems to be the craze on TikTok at the moment, we have found (last week) videos/bogus school accounts that have been created, which have used Staff photos/videos from our website/Google image search, with some very personal comments over the videos. My own photo has been used, along with other male staff and our Headteacher, with reference to Paedophiles and other derogatory comments.

The Senior Leadership team are also involved in attempting to identify the publishers of this material.

As yet (one week on), all the videos and accounts are still live. TikTok never respond, despite numerous staff here regularly reporting the accounts and videos, and we are unable to get them taken down.

The links are below, but a search using our school name brings up these videos and some accounts:

{url}

{url}

{url}

One account in particular:

{url}

You'll see some new text in the Biography heading (put live this weekend) once again targeting our Staff/Teachers.

Are you able to assist in getting these wholly inappropriate videos removed from TikTok?

CYBER-BULLYING

Questions related to online abuse directed at either staff or pupils in a school setting.

We have spoken to two students this morning who are very distressed by two social media accounts that have been set up to bully and intimidate them. Both were reported and whilst it appears they have been removed, it is unclear whether this is a temporary or permanent removal. Is there any way to find out?

Also, do you have any advice about how to find who set them up (presumably the social media companies have IP addresses etc that would link accounts??). The police have been informed and they are coming in this morning. Any further advice you can provide would be appreciated.

The Twitter handle is {{username}}

The Instagram accounts is called {{username}}

Please see attached email from {{School}} highlighting an Instagram account called {{username}} and photos of a young female student of the school which have been posted on the Instagram account without her consent. The female in question has complex mental health issues and the posting of these photos could cause her severe anxiety and lead to self harming.

Can you assist to get the posts removed, the account closed or offer any advice?

I'm a primary teacher and recently have had unwanted messages on Twitter. They're from anonymous accounts but are clearly from an ex-colleague who didn't like me. One account made comments generally about the school we both used to work at (staff being toxic, terrible place to work etc) as well as personal things about me and what a terrible teacher I am. My friends and I blocked the account so heard nothing else. That was at the end of half term. Then last Thursday I had a DM from a different account asking for curriculum support (which I do offer quite often). I thought nothing of it but they asked for my email address, then blocked me without getting the help they were asking for. I think it must be the same person trying to work out which school I work at now from my work email.

I've blocked and reported, but is there anything else I can do?

POTENTIALLY HARMFUL CONTENT

Concerns around content that requires investigation or advice regarding its potentially harmful nature.

We would like some help and advice on how to support a Year 6 pupil who has divulged information about his use of the internet.

Some of this use has been more historical and some more recent. We have other staff involved including a police mentor and from school – the head, deputy, SENCO and pastoral team. The school have applied for an EHCP. He recently has a diagnosis of Autism.

The online concerns we have cover:

- accessing porn and speaking about it to his peers (in year 5)
- accessing games above his age
- accessing YouTube to watch how to 'hack' (his words) into games to change what he can do, levels to play, content he can access (we think he really means applying cheat codes)
- accessing YouTube to find out how to hack into webcams
- accessing YouTube to know how to change his location so that he cannot be tracked – he said he tried this but the account was then shut down
- he created a game on Roblox for Russia versus Ukraine and uploaded an image of a Russian soldier with a gun – he said his account was blocked for a week
- he claimed he could change prices on Amazon then admitted that although it changed it went back to normal and couldn't buy it.

A PREVENT referral has been made and our SENCO is liaising with the local police on this and a MASH referral is to be made. Another Early help referral has been completed as a triple P parenting referral.

Is there currently an online TikTok trend for young people posting videos of themselves holding knives and saying 'don't touch my friend again'?

I work as a Liaison Nurse in the children's safeguarding team

I screen all paediatric ED attendances and have observed some recent themes of concern where children have become injured or unwell after recreating video "trends" from social Media sites such as TikTok and Facebook.

POTENTIALLY HARMFUL CONTENT (Continued)

We have had a number of attendances following engagement in the following activities:

"Choking game"/choke holds where children are essentially strangled for as long as possible and/or until they "get high" (or pass out).

Spraying own/others' skin with aerosols for as long as able to tolerate. Often sustaining aerosol burns .

I hope this information can be helpful in seeking ways to limit the availability of such content online.

WEBSITES

Enquiries that relate to problematic content on other websites such as blogs, or website hosting issues.

I wondered if you might be able to offer advice for village halls who wish to support digital inclusivity and provide internet connection to their members.

Our village hall has recently had broadband installed. Having recently joined the other volunteers of the committee, I would like see the use of the Wi-Fi being offered to the members of our village club.

The committee have concerns from a safeguarding point of view, surrounding children and vulnerable adults. There are also concerns that the committee could be liable should someone use the hall's internet connection in an inappropriate manner.

We would like to provide internet access for our members, in a safe way for all users. I have been tasked with writing policies and was wondering if you have any policies or written terms of use, that you might be able to share with me, please.

I am trying to access the 'gone too far' worksheets for the cyber-bullying lesson. I have the lesson plan and the PowerPoint presentation but cannot seem to access the worksheets and the link to the toolkit does not seem to be working.

Any help with this would be much appreciated!

WEBSITES

(Continued)

I'm emailing to ask if you had any additional information about online challenges?

I have heard from colleagues over the weekend who are worried about an article shared on Distractify which details a yearly calendar of online challenges (see below). I was wondering if you could help me substantiate these challenges. As yet I have not been able to verify them, and it is becoming a source of anxiety for colleagues.

- September: Vandalize school bathrooms
- October: Smack a staff member
- November: Kiss your friend's girlfriend at school
- December: Deck the halls and show your balls
- January: Jab a breast
- February: Mess up school signs
- March: Make a mess in the courtyard or cafeteria
- April: Grab some eggz (another stealing challenge)
- May: Ditch day
- June: Flip off in the front office
- July: Spray a neighbor's fence

TECHNICAL SETTINGS

Advice about the use of platforms, privacy settings, security controls, etc.

Question about DBS – school want to have a guest speaker – they can talk remotely in the classroom via the schools VLP, and do not have any direct contact with students – do they need DBS? Advised it doesn't sound like they technically do but we would advise it is good practice, recommend getting the application done ASAP and while that goes through the guest speaker can talk via VLP with the teacher in the room.

Hi

Do you have any advice for schools wishing to present to parents a live streaming event via YouTube?

In this case it would be an Online Safety session in conjunction with Police on 27 January 2022.

TECHNICAL SETTINGS

(Continued)

We wish to schedule the live event and share the event via a link. We have an unlisted YouTube channel that we have previously used to share nativity play etc. It seems I also need to download software. I was looking at downloading Streamlabs.

Does this seem OK to you and can you share any other help?

I was hoping for some advice. We have 1:1 devices and we have filtering and monitoring software on the devices. The devices are owned by the school and the students take them home in the evenings, weekends and holidays.

A question has arisen if the monitoring picks up a safeguarding issue in the evening or weekends or holidays who is responsible for this?

- Is the school responsible and needs to act on these alerts 24/7, effectively having a DSL monitoring all the time?
- Can the school dictate that any alerts are dealt with next working day?
- Is the parent/guardian responsible as even though it is our device they are in their care at the time? If so, we could disable monitoring offsite/at certain hours as the school is not responsible, the device would still be filtered.

Any advice or comments would be appreciated.

REPEATED HARASSMENT

Enquiries based around harassment of staff and students in schools.

In the last couple of days 2 accounts have appeared naming themselves the school which have uploaded videos of teachers' images taken from the school VLE in many cases created videos accompanied with unkind lyrics. They have then tagged pupils in and proceeded to make unkind comments about the staff. I am one of the targeted members of staff.

I have reported both accounts to TikTok and I have reported each video for bullying and harassment, this was about 20–24 hours ago and there hasn't been any response from TikTok at all. The Headteacher has also reported to TikTok 2 days ago and hasn't had a response either.

REPEATED HARASSMENT

(Continued)

Please delete this account. It is posting pictures of school children and videos without their say so. Including my daughter who is suffering mentally because of this.

My main and only email, where I have emails from the police, solicitors regarding this abuse to me including sensitive personal information about trauma and abuse I suffered as a child from supportive organisations. My password has been changed and I have been locked out of my account.

This is very upsetting and distressing and making me more suicidal and depressed. I need this abuse and hacking to stop.

SEXTING

Enquiries related to incidents of the non-consensual sharing of intimate images among peers.

I am not sure if you can support in this matter. A child in year 8 at our school has shared an image of herself on a private Instagram story. In it, she is wearing some quite skimpy shorts. The image has been shared amongst the year group.

We work with the young people involved, as best we can, to speak to them about the consequences of this sharing. We also support the child whose image is being shared (her parent is aware and working with us).

Is there anything that you are able to support with to help prevent further sharing of the image?

Issue is girls at school are reporting being sent nudes constantly from boys at the boys school near them, they say there is no point in reporting it as it happens ALL the time, teacher feeling frustrated that these girls have seemingly nowhere to go and nowhere to report what is going on, she said they can tell 'everyone's invited' but this isn't a solution.

SEXTING (Continued)

I have a query regarding a situation where a child has been dared to send an explicit photo of himself to a group chat. He has done this and then deleted the image, but another person in the group chat has saved it and sent it to some other people. There are 3 people who we know definitely have the photo.

We have spoken to the student who sent the image who understands why this is wrong and that it is a criminal offence. Our plan is to now speak to the 3 boys who have the image, sanction them according to our behaviour policy, and speak to parents. We do not feel it is necessary to call the police, however, wanted to check this with you first as the DfE guidance is not completely clear.

MEDIA LITERACY EDUCATION

Enquiries that are asking for advice related to issues of media literacy, such as signposting for online safeguarding resources, policies and training, and questions about the use of different technology in professional settings.

Hi there,

We have a member of staff who needs to talk with a Romanian parent about her child's searches on Google found on our Monitoring system.

Do you have any translated guidance that we can use to help us or that we can share with the parent?

I am working with a young man with a Significant Learning Disability who I have assessed as not having Capacity to manage free access to the internet and social media due to his inability to anticipate, avoid and respond to associated risks and I am considering the need to install a Parental Control App to his devices in order to monitor and protect him from being targeted (as he has been in the past). I would value any best practice advice you can give me on this matter in terms of how to frame the support agreement/contract he needs in order to keep him at the centre of the arrangement as well as any guidance on the merits of using one or another of the Parental Control Apps on the market.

I work in a science education centre and we are looking to set up a mentoring programme with school students (14+) as mentees and university students (18+) as mentors. We are thinking of having the mentoring sessions online, with university and school students setting their own times. Online mentoring is new for us and I was hoping I could speak to someone to understand how we should adapt our safeguarding practices?

SEXUAL HARASSMENT

Enquiries related to sexual harassment online and supporting professionals who are supporting young people who have been subject to harassment.

Is there up to date advice on cyber flashing?

And do you agree this should be included in Policy and resource response to sexual abuse and sexual harassment in schools, alongside sexting and upskirting?

Can you advise myself and my safeguarding colleagues.

One of our schools has been contacted by telephone by someone called {name}. The person had seen some girls at the school on TikTok and the associated posts had inappropriate comments about tight skirts etc. The person then emailed screenshot to the schools. They were indeed genuine screenshots and the girls did attend the school.

I have advised the school that this is a self-appointed vigilante organisation (the format of the email indicates that it its not an official group) and have warned against divulging any information although this was not asked for. I have explained that the groups are staffed by self-appointed, unvetted volunteers and that however well meaning some of the individuals might be, there have been some cases of long-standing police investigations being put into jeopardy.

A young person in our setting (13, special needs and I believe has no capacity to consent) has been filmed having a threesome with two males slightly older than her. Another young person in our school said to a staff member, "look at this sir it's not right".

The staff member did see the video for a second or two and has come straight to SLT to report the concern.

The young person involved is not in today but lives very close to school.

We are going to call the police but wanted advise on if there are quicker ways to stop the video being online and if we should go and speak to the girl (two staff with parental permission) to see if it could be her, if she knows who it is and if she is happy to talk to the police?

DATA PRIVACY

Concerns related to privacy and data protection.

We have a Year 10 student who was contacted on her snap and said look at your Instagram because I have hacked it. He has changed her user name and password on Instagram and blocked her on snap. The hacker is now sending messages to her and her contacts asking for nudes and money and saying that he {{name}} give her account back if she sends nudes.

I am hoping you can advise me over some alerts that three of our Year 9 pupils have received on their mobile phones. They are getting alerts saying that an air tag is tracking them and knows their location. The first alerts came through while they were on a trip to the bowling alley on Saturday 27 November (last night). The alerts have been coming in fairly regularly since then and when you open the alerts you can see that there is a map with their location on, tracking them from the bowling alley back to their boarding house.

Please can you advise me over how we can block and stop these alerts? As a boarding school we are very mindful that our school site is open and that the tracking map shows the location of our boarding house, which houses 70 girls.

My account {username} on Instagram has been hacked and my email, contact number have been changed. In addition to this I then received the attached message requiring action from me in order to gain access to my account. My account was registered using the email: {email address}

LOVE, RELATIONSHIPS AND SEXUALITY

RSE related questions that have an online element to them.

Hi, I have someone threatening to leak a private video of me that I sent to them on Snapchat and I was wondering if there is any way you could help me get the video deleted

A 15 year old student (named X for purposes of anonymity in this email) has admitted to sharing images, videos and video calls with someone they have never met via social media. Both parties have shown images of their naked bodies and masturbation. X says this was fully consensual. X said their face was not included in any of this imagery. Both parties checked the other

LOVE, RELATIONSHIPS AND SEXUALITY (Continued)

wanted to be part of this situation. X met this person online and believes the other person involved is the same age, they believe this because they have been on Facetime to them in school uniform. X told me they have no plans to meet the other party, but has asked mum if they can meet during the holidays.

X's mum confiscated their phone, when she walked in on X masturbating on Facetime to this other person. X is unsure as to whether there are any unsolicited images on their phone as these were sent over Snapchat and X isn't sure if they were saved. I have advised mum to take the phone to the police if she is in any doubt of who this person is, in order to safeguard her child. Mum has not done this yet.

Can I check whether there is more that I should be doing as a school? X has attended online safety lessons in schools and is fully aware of consequences but has continued to make this choice. Any advice you could give me or mum on next steps would be appreciated.

E-CRIME

Specific enquiries related to illegal activities online, such as those who meet legal thresholds for abuse or illegal content.

I am being blackmailed – how do I stop it? I'm 59 years old and I want to stop it.

Two of our teaching staff have had abusive messages sent to them from the outlook.com address below. They were highly offensive and pornographic in nature. Due to some of the content being directed at staff by name, we believe they were sent by a student.

However, as the address is an outlook.com account, and from an analysis of our systems they weren't sent from a school computer we are unable to identify them.

We've blocked the address below from our email system but was wondering if there is anywhere we can report it to try and identify the perpetrator. Due to the offensive nature of the email we will also be reporting it to the police.

Any advice/direction you can give me would be much appreciated. Thanks

E-CRIME *(Continued)*

I was silly enough to fall into a bitcoin scam, my Instagram account has been taken over. I'm not in control of it anymore – could I have it removed please?

They are scamming my family and friends and I need it stopped as a matter of urgency.

BIBLIOGRAPHY

1 <https://swgfl.org.uk/services/professionals-online-safety-helpline/>

2 <https://swgfl.org.uk/training/online-safety-live/>

3 <https://swgfl.org.uk/services/professionals-online-safety-helpline/>

4 <https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022>

5 <https://bills.parliament.uk/bills/3137>