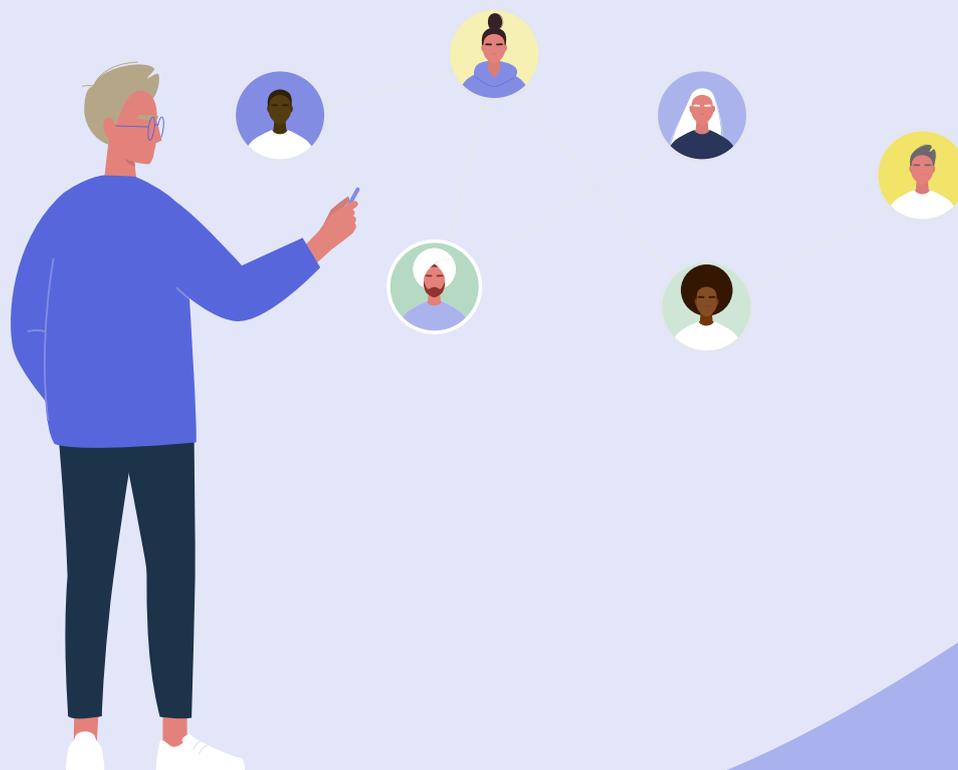


Online safety: health, education and law enforcement workers

October 2021



Contents

eSafety research program.....	2
Overview.....	3
Key highlights.....	4
Findings.....	7
Experience with clients' online safety issues.....	7
Perceived role.....	14
Barriers in dealing with online safety issues.....	16
Barriers in dealing with engagement.....	23
Support needs.....	25
Conclusion.....	26
Methodology.....	28

eSafety research program

The eSafety Commissioner (eSafety) supports, encourages, conducts and evaluates research about online safety for Australians. The eSafety research program tracks trends, collects, analyses and interprets data and uses this to provide an evidence base for the development of eSafety resources and programs. eSafety also works closely across agencies and internationally so that its research program can proactively identify and explore online safety issues. eSafety makes all its research publicly available via its website esafety.gov.au/about-us/research

For any enquiries about the eSafety research program, please contact research@esafety.gov.au

To register for the latest eSafety news, including research, subscribe at: esafety.gov.au/about-us/subscribe

Overview

Frontline workers in the health, education and law enforcement sectors provide essential services directly to the public and they often find out about online safety issues through the course of their work. This means that they have a unique opportunity to play a role in supporting their students, patients or clients through online safety issues.

This research was conducted to explore frontline workers' experiences and perceptions of online safety and to gain an understanding of the resources they need to effectively assist their clients in accessing further support.

The research involved 18 in-depth interviews with professionals working in health and welfare (general practitioners, nurses, psychologists and youth workers), 30 interviews with education professionals (early childhood, primary school and secondary school settings) and 16 interviews with law enforcement professionals.

The research found that there were a number of systematic barriers that participants faced when assisting their clients with online safety. These included a lack of knowledge of online safety issues and a lack of access to resources.

Participants demonstrated an awareness about the online issues their clients experienced, with the most common being cyberbullying, image-based abuse, technology-facilitated abuse in the context of domestic violence, unwanted contact and excessive technology usage.

The ability to take action differed across the professions. For example, participants from the education sector were more alert to online safety for children and young people than other frontline professions. They were also more familiar with online safety incident prevention and management as it forms part of their role.

This research highlights that there is an opportunity for frontline workers to be empowered to assist clients with online safety issues. This includes through developing practical resources such as simple fact sheets and guides to action which would assist them to build awareness and understanding of online safety.

Key highlights



Experience with clients' online safety issues

- Frontline workers encounter a broad range of online safety experiences that impact their clients, ranging from too much screen time to cyberbullying and online abuse.
- The nature and level of clients' online safety issues varied greatly by occupation, for example:
 - general practitioners (GPs) had typically come across a limited number of online safety issues
 - allied health professionals and law enforcement officials identified a range of issues they had come across through the course of their work
 - educators, due to their work with children, young people and parents, were more likely to be exposed to a broader range of online safety issues and more often.
- The circumstances in which frontline workers are exposed to the online safety experiences of their clients is mixed, for example:
 - some educators were aware of issues and had heard about them directly from students, others had learned of issues through observing behaviour or by word-of-mouth
 - health professionals and law enforcement heard directly from clients and interviewees through the course of their work.



Perceived role

- There were marked differences in the ways that frontline workers perceived their role in supporting their clients' issues with online safety:
 - early childhood and primary school educators saw themselves as having an active role in ensuring the wellbeing of children, while secondary school educators typically had a stronger focus on academic achievement

- GPs generally had a narrow and highly medical approach
- youth welfare, sexual health and maternal and child health professionals were aware of the potential vulnerability of clients therefore considered broader wellbeing
- law enforcement officers working in general policing typically viewed online safety through a tight frame focusing on evidence gathering or the potential for prosecution.
- Frontline workers' perceptions of their role in online safety are shaped by a range of factors, including:
 - the extent to which technology is integrated into a client's life
 - the extent to which the client understands the risks of technology and how to protect themselves
 - whether their clients are exposed to age-appropriate content
 - whether mandatory reporting applies
 - whether police investigation and convictions are possible.

Barriers to engagement with online safety issues

- For many of the professionals interviewed, their lack of personal experience, understanding of technology and knowledge about online safety limited their ability to identify issues. It also limited their capacity to prevent or manage online incidents.
- Many frontline workers have a low level of confidence dealing with online safety issues. This can be for a range of reasons, including online safety not being viewed as a core part of their profession, lack of technical expertise and being unable to keep up with technology.
- Most frontline workers agreed that it is hard to identify when an online safety incident is affecting a client, or if there is another reason for their behaviour.
- Terms such as 'online safety', 'image-based abuse' and 'technology-facilitated abuse' are not intuitively understood by many frontline workers. Other terms like 'sexting' can be understood by people who work with teens but are unfamiliar to other professions. Terms frequently used in the media like 'cyberbullying' and 'revenge porn' were more likely to be understood.

- During the interviews, most frontline workers said that they had become more interested in online safety. The research identified that there is demand for setting-specific training and resources, that tailors information for different occupations.

Resource and support needs

The research found that frontline workers need practical resources to address their knowledge gaps and to increase their engagement with online safety issues. This includes training and resources that are specific to their setting with options such as:

- training opportunities to help increase frontline workers' self-confidence in dealing with online safety issues
- providing a map of the online environment in the form of a 'cheat sheet' highlighting where online harms can occur, the risks involved, signs of impact on clients, and available referrals and support services
- developing practical health pathways, relevant to individual settings
- providing investigation 'cheat sheets' for law enforcement professionals
- developing a decision process to help frontline workers guide clients to further support
- developing resources that frontline workers can pass on to clients and their parents.

Findings



Experience with clients' online safety issues

The research found that the level of engagement frontline workers have with clients when looking at online safety issues varied widely – ranging from limited experience with online safety, to actively supporting clients through an incident. Nurses and allied health workers, for example, had limited exposure to online safety issues in their work, whereas primary school and early childhood educators had experience in supporting students, talking to parents and using technology as an educational tool.

Participants from the health and education sectors encountered online safety issues only when they were reported or disclosed to them by patients or young people in the health and education professions. Those from law enforcement became aware of issues if a member of the public reported an incident presented at a police station or, in the case of specialist police such as those working in domestic violence or sexual crimes units, if an incident was referred to them.

Early childhood educators and primary school educators heard about online safety issues through children telling them directly, by overhearing children talking about something they had seen or heard, or by observing certain behavioural changes in children and finding that an online incident was the trigger.

Notably:

- GPs had typically come across a limited number of online safety issues in professional practice. Specific examples given in the research showed they encountered these by:
 - Treating young people presenting as socially withdrawn or anxious, having trouble concentrating – and discovering they were being cyberbullied on social media. GPs would hear either directly from a young person about their experience or from parents seeking support about how to manage cyberbullying.
 - Patients disclosing identity theft and online fraud in the context of having their Medicare card stolen.

- GPs observing children, young people or even adults spending most of their time on screens in the clinics and being concerned about the impact of excess screen time on patient wellbeing.
- In some isolated incidents, patients raising pornography addiction and technology-facilitated abuse by an ex-partner during consultation.
- A mother raising a concern that her daughter was being groomed in an online chat room.

Case study – GP case study

Anaya works as a GP in a long standing suburban medical clinic. Most of her colleagues are older. She is known for her interest in technology and her connection to her teenage and female patients. Anaya has had both young people and their parents disclose cyberbullying incidents to her and feels a deep sympathy for them.

Anaya believes that cyberbullying can have a significant impact on young people's sense of self-esteem and mental health however sees it is a very difficult area to manage as a GP. When a distressed and disturbed young person comes to her, there is little she can do to gauge the nature of the problem or effectively address it in a 10-minute consultation. Referring on to a psychologist, or a support service such as Kids Helpline is the best she can do.

However, Anaya thinks she is probably doing more than most of her colleagues, in even considering online safety as a potential cause. She argues that a health pathway¹ to help identify issues, as well as short resources and referral phone numbers that can be easily passed on to patients, would be helpful in having more GPs engage with the topic.

Anaya helps run GP training through her local Primary Health Network² and would love to help facilitate a session on how GPs could consider online safety in their practice. However, she realises that less engaged GPs are unlikely to attend these sessions. Information that reaches GPs in their workplaces, for example, through placement in GP publications that everyone reads (Australian Doctor, Family Physician) will be important.

- Psychologists were easily able to list the online safety concerns raised by clients during their professional practice. For example:
 - The telephone-based psychologist had heard about the negative impacts of cyber stalking, online harassment, catfishing and financial

¹ A health pathway is an online resource for GPs to use at the point of care. It provides information on how to assess and manage medical conditions, and how to refer to local specialists and services.

² Primary Health Networks are regional organisations, established and funded by the Commonwealth Government, with the aim of increasing the efficiency and effectiveness of medical services and improving coordination of care.

scams on clients' mental health and wellbeing; and one client's legal exposure because of sending visually explicit images.

- The child psychologist talked about cases where children had experienced cyberbullying and too much screen time, and the subsequent impacts this had both on their relationship with parents and peers, and childhood obesity.

Case study – psychologist

Anne recently qualified as a psychologist. She is IT savvy and feels comfortable talking about gaming, different social media applications and the potential for online safety incidents to impact her clients.

Anne works for a community service and rarely sees clients on an ongoing basis. This means that she often isn't able to provide prevention-focussed information and education to clients. The exception to this is when clients talk to her about proposed actions that might expose them to online safety risks and she can advise them to be more cautious. For example, she warned a young person wanting to engage in sexting, and an older person who was reaching out to strangers for help managing online transactions, that they needed to be careful with their choices. She is highly aware that the impacts could be serious, such as being charged with a criminal offence or having personal information exposed and misused.

Anne also supports distressed clients and so is highly aware of the detrimental impacts of online safety incidents (such as cyberbullying and technology-facilitated abuse) on mental health and social and emotional wellbeing. However, the limits of her setting means she can't support patients in the long term. Her key needs are for information and referral pathways so that she can support clients to seek ongoing help as they manage online safety incidents.

- Nurses heard about issues directly reported by their patients and clients or by observing patients and clients at appointments including:
 - maternal health nurses hearing from new mothers about cyberbullying they experienced through Facebook groups
 - children under the age of five being observed at maternal and child health appointments as being vulnerable to online safety risks and exposure to excessive screen time (based on access to screens during appointments)

- maternal and child health nurses observing controlling partners using online content or technology as a means of exerting control in family violence settings.
- Youth workers had either observed issues or received reports including:
 - young people sharing information online that exposed their location and their personal information to predators
 - reports of online harassment, including in a family violence context, and peer bullying
 - young people with a cognitive impairment not realising the implications of posting online such as not being aware that their content is being made publicly available.

Case study – youth worker

Loc is an NDIS support coordinator with a number of young clients living in group homes. His job is to work with clients to help them connect with services as part of their NDIS plan. While Loc regularly sees his clients and has strong relationships with them, he feels like he doesn't have much control over their online lives or ability to monitor what they are doing online. All have digitally-connected devices, and Loc imagines that the older teens and young adults – who use social media to send around images and contact people online – may be vulnerable to predatory strangers online (although he hasn't observed this himself).

However, while Loc sees the risks, he doesn't believe that he is the right person to intervene in online safety incident prevention and management. He says that disability support workers who staff group homes would be in a much better position to protect and support young people on a daily basis.

This would require the NDIS service provider (who employs disability support workers) to adjust their worker training and resourcing.

- Technology was seen by law enforcement professionals as an increasingly common aspect of policing. The range of issues that they had come across at work included:
 - cyberbullying through use of cruel and threatening language via social media, and filming and sharing violent incidents in order to shame/harass another young person

- image-based abuse where intimate images were shared without another's consent
- technology-facilitated abuse in the context of family violence including stalking/surveillance via 'tracking' and 'ghosting' apps and CCTV, hacking email, bank and social media accounts, controlling, manipulation, and sending threats and abuse via emails or social media.
- Early childhood educators typically knew little about the range and extent of risks the children in their care could be exposed to. Some of the issues they raised included:
 - exposure to inappropriate content where children or parents/carers talk about an experience that has disturbed them, or educators observing behaviour such as too much violent play, obsessive references to screens etc. and identifying the trigger as a negative online experience
 - children telling educators about having personal communication with strangers via online games or social media platforms e.g. Fortnite and Snapchat.
- Primary school educators were most alert to the dangers and impacts of connected device use. For example:
 - Cyberbullying was seen as more prevalent in the latter years of primary education (years 3+) where educators report that cyberbullying occurs on social media such as Instagram, either through family accounts or a child's own account (in years 5–6+), as well as through interactive gaming.
 - Interactive gaming was another area of concern where educators observed and heard about students playing online games. Educators noted that children play online games through all primary age groups, but independent play tends to start upwards of age 6. The most frequently mentioned game was Fortnite, which facilitates interaction with strangers. There is a concern that parents are not aware of this element of the game.
 - Excessive screen time was a particular area of concern for educators based on extrapolation. Educators were concerned that some parents were not monitoring their children's time online and children were subsequently accessing inappropriate content, including age-inappropriate social media, pop up ads and pornography.

Case study – primary school educator

Michael is in his fourth year of teaching and teaches a grade 5 class in a government primary school. He is passionate about his work and loves teaching at a school that has a progressive focus on inquiry-based learning and a positive, strengths-based approach to children's social and emotional wellbeing.

Michael is concerned that children's use of digitally-connected devices is exposing them to issues that they aren't equipped to deal with. Cyberbullying is emerging as an issue for children at younger ages, and he perceives that children's excessive screen time and adoption of age-inappropriate games (such as Fortnite) are having large impacts on children's engagement with education as well as their social and emotional wellbeing.

When issues arise, Michael works closely with the school's wellbeing team and leadership to resolve them. However, he wishes his school addressed prevention, as well as 'putting out fires'.

Michael has previously taught at schools with comprehensive online safety incident prevention and management systems and is lobbying his Assistant Principal to adopt the same.

He is doubtful about the effectiveness of parent education. It's important, but Michael notes that it is always the same engaged parents turning up to information and education nights. He believes that the families that need the most support – and where children are most at risk due to their parents being vulnerable or otherwise being unable to supervise their children – are less likely to voluntarily come to school to learn about issues such as online safety. He is not sure where the solutions lie and believes that this should be an ongoing focus for eSafety.

Michael would like his school to develop clearer guidelines and policies around the safe use of technology in school, and incident management. He would also like to be provided with online safety prevention resources that address the issues his year 5 students are experiencing, and that are age and developmentally appropriate.

- Some secondary educators raised specific incidents that emerged through their connection to an individual student (including students who

volunteered details about issues). Others' knowledge was built through school word-of-mouth and gossip. Some of the issues include:

- Cyberbullying via social media (particularly Snapchat) with reports of students being nastier and more forthright than they would be in person, noting that online access also means that bullying is 'always on' so a student can't escape after school hours.
- Sexting, as a major concern. This was felt to be highly prevalent across all age groups. It included situations where young girls reported that older boys threatened them and demanded they take naked pictures of themselves.
- Concerns about students' digital footprint were based on what educators knew about the issue and students. Educators felt that young people are not as aware as they should be about their digital footprint.
- Harassment of staff – some educators mentioned personal experiences of cyber abuse from parents or students. This includes through unmoderated websites such as 'Rate my teacher' as well as on social media.



Perceived role

There was a marked variation across frontline workers about whether their professional setting enabled them to take a holistic approach to the wellbeing of their clients. For example:

- Early childhood educators and primary school educators take a highly active role in ensuring the wellbeing of children. Early childhood educators also believe they have an obligation, not just to the child, but to their whole family.
- Secondary school educators typically have a stronger focus on academic achievement than the overall wellbeing of their students unless they have a welfare or coordination role. They are less likely to see the family unit as being a part of their role.
- In the health sector, issues raised by clients tend to shape the scope of engagement. GPs can have a narrow, highly medical approach. In contrast, youth welfare, sexual health and maternal and child health professionals are aware of the potential vulnerability of clients and patients, including in the

context of mental health and family violence. This means they also consider comprehensive social and emotional wellbeing needs.

- In law enforcement, officers working in general duties typically work within a tight timeframe and view online safety issues in light of the potential for prosecution.

Table 1: Frontline workers and perceived online safety role

Profession	Overall focus	Perceived online safety role
Education		
Early childhood educators	Education and wellbeing	Frontline workers believe that their young students have to adapt to a world that involves more technology. But they are cautious about how technology is used. This underpins a desire to be better informed and a willingness to take on a key role in proactively and responsibly helping children prepare for, and successfully navigate, their digital future.
Primary school educators	Ensuring wellbeing and safety of students	Most participants feel that technology and connected devices are important tools in education. They focused on mindful use of technology and showing students how connected devices should be used with purpose.
Secondary school educators	Academic achievement with a student support role	Secondary school educators' awareness of online safety issues varies in line with the subject matter they teach. They have a supportive role but when it comes to online safety incident prevention, most feel students know more about the world online than they do.
Law enforcement		
Police officers	Evidence gathering/potential for prosecution and physical safety	Law enforcement workers focus less on online safety prevention. Most perceive that this is a role for specialist education units. Workers in specialist units, where family violence is involved, are more likely to see online safety as a core part of their role.
Health		
GPs	Strong medical focus	Most GPs feel they have a limited role in prevention of, or response to, online safety incidents.

Profession	Overall focus	Perceived online safety role
Allied health including counselling, support services and nurses	Mental health and wellbeing approach	<p>Psychologists' approach to online safety is informed by their varying clinical contexts and patient base, as well as their own familiarity with technology.</p> <p>Maternal and child health nurses tend to see online safety through the lens of larger issues, for example, loneliness, maternal mental health or parenting ability.</p> <p>Nurses also see online safety as a workplace issue, because of staff bullying each other online, for example.</p>

Given the perspectives detailed above, some frontline workers may not have considered online safety issues as relevant to their work. This research suggests that there are opportunities for some professions to play a more active role in identifying these issues and assisting clients.

There were some exceptions to the broad perceptions summarised above, with some frontline workers having a profound interest in the wellbeing of their students, patients or clients and pursuing this regardless of their professional setting.

Barriers in dealing with online safety issues

The research identified a number of barriers frontline workers faced when dealing with their clients' online safety concerns. While these workers expressed a strong duty of care for their clients' wellbeing, there were several reasons they may not have been well equipped or well positioned to intervene in online safety issues.

Frontline workers noted that limited knowledge of how online safety risks and impacts might apply to their clients, a low sense of self confidence and the lack of a practical tool kit are strong barriers to action on online safety issues.

Their perceptions of online safety interventions are shaped by the how they view their clients including:

- **How technology is integrated into a student, patient or client's life**

For preschool and primary school children, online safety interventions focus on putting up boundaries and separating young children from risks posed by technology. However, as children grow, become teens and then adults, online experiences become interwoven into their lives and more clearly

contribute to work, education and social benefits. As online experiences become more complex, the role online safety interventions play also becomes less clear.

- **Clients' understanding of the risks of technology and how to protect themselves**

Preschool and primary school educators believe that focussing on prevention for, or intervening in, an online safety incident is complicated because very young children are not capable of understanding the concepts involved. They expressed fears, for instance, that children might not understand the nuances of 'reality' online, including the need to be kind to friends online – as one might in real life. Also that strangers might not be as they seem and that not everyone online is a friend. To help build their confidence, it is important to reassure these frontline workers that developmentally-appropriate interventions are available.

- **Age appropriateness of explicit content**

Educators are interested in age-appropriate content – they are aware that parents might not approve of curriculum materials that introduce sexual content, or other concepts, that parents believe their child is too young or naïve to see. The Safe Schools and Respectful Relationships programs were given as examples of where this had occurred. Supporting educators to successfully engage with families is an important consideration when developing resources.

- **Whether mandatory reporting applies**

The mandatory reporting obligations that apply when frontline workers believe children to be at risk provide a clear role and standard for intervening in online safety incidents involving children. By contrast, the standard for intervening is less clear cut for those who deal with adults or teenagers. Frontline workers can be reluctant to engage intrusively with older clients as well as in cases where their role is less clearly defined.

- **The extent to which police investigation and conviction is possible**

Law enforcement professionals noted that the limited capacity of cybercrime units and uncooperative social media companies constrains their ability to act.

In addition to how their clients are viewed, the research identified personal barriers that impact on frontline workers' ability to prevent or manage online safety incidents for their clients.

1. Lack of personal experience and understanding of technology

Frontline workers' ability to prevent or manage online safety incidents is, in some cases, limited by low knowledge of technology and online environments. These workers typically engage with online safety based on their personal experience and knowledge. Being a parent (which encourages a greater focus on online safety, especially as it applies to children) and the extent to which frontline workers see themselves as being 'tech savvy' make for a stronger sense of commitment.

'And I am interested in it. Only because I've got two small kids and I've actually just, it's really concerning as a parent. And also as a psychologist, and seeing how it does impact on a young child's life.'

Psychologist

This personal lens is often very narrow, resulting in frontline workers not understanding the full range of technology used by students, patients and clients, the potential for risks and the need for action. Notably:

- Workers can mistakenly believe that certain issues are not relevant in their context or for their clients. Early childhood educators, for instance, could believe that children of preschool age wouldn't be exposed to inappropriate content online. Because they don't see the risks, they then don't see the benefit in acting.
- Workers appear less likely to see impacts if they have limited knowledge of online activities – they don't know/aren't alert to signs that an online safety incident has occurred, and so don't intervene to offer support – even if they are positively disposed to action.
- High profile online safety issues tend to dominate workers' perception of what online safety incidents might be likely or even possible. Screen time, cyberbullying and issues affecting children and young people are the focus of media coverage and existing prevention interventions in schools. This appears to be at the cost of thinking about other issues such as inappropriate content, exposure to online predators (for grooming and financial or romantic scams), maintaining online privacy/control of personal data and adults' experiences.
- The default is to consider issues affecting children and young people. In interviews where frontline workers deal with adult audiences, frontline

workers needed considerable prompting to focus on adults' needs. This indicates a need for communication and resourcing to reinforce this focus on adult online safety.

2. Low sense of self confidence

Many participants were not confident in dealing with online safety issues. This is for a number of reasons including:

- Online safety isn't a core part of their professional expertise.
- They don't see themselves as 'technical' people.
- Ongoing advances in technology can feel unstoppable – frontline workers rationalise that there is little they can do to halt this progress, nor do they want to, given the potential benefits of technology.
- Technology, and interactive online channels such as social media and online gaming, are always evolving – a lay person can't keep up.
- Online safety issues are outside their control. Incidents do not occur in their work settings, except for secondary school and young people living in group homes. These incidents involve a number of complex aspects of a student, patient or client's life. For example, the incidents can be due to actions of third parties or they are so pervasive that workers can feel they cannot possibly have an impact (such as sexting or teenagers accessing porn).
- They believe that younger people are much more tech savvy – there is little that they can say that will be listened to by their younger students, patients or clients.
- They haven't been trained in, or resourced to handle, online safety incident prevention and management.

As a result, frontline workers can easily disengage from online safety. If they do engage, their instinct can be to refer onwards at the first possible opportunity. Increasing workers' sense of self confidence will be key to increasing engagement and action.

'So, if it happened, would probably tell the nurse manager, and then Google to see if there were any resources I could find to help them, or get some advice on how to handle it.'

Nurse

3. Online safety incidents seen as a 'grey area'

In the early childhood sector and in the first years of primary school, a high proportion of educators were sure that they could identify the impacts of too much screen time in young children. However, beyond this, most participants agreed that it is hard to identify when an online safety incident might be affecting a student, patient or client. For example, a child exhibiting behavioural issues could be having a difficult time at home or in their education setting, they might have an undiagnosed mental health condition/disability, or they might be being affected by something they have experienced online. Educators, GPs and allied health professionals agreed that, in this circumstance, a paediatrician, psychologist or psychiatrist would need to explore the issues further – they were not equipped to diagnose.

Similarly, participants felt they often wouldn't know whether an online safety incident was a contributor to an adult presenting with distress or describing themselves as being in difficult circumstances including involving family violence. Again, the instinct of most workers is to refer on, rather than deal with the issue themselves, or to dig deeper to understand if online safety issues are involved.

'With image-based abuse – if I thought they were a victim or even the perpetrator, I'd definitely say something to the nurse manager, I wouldn't let it go. I don't know what'd I'd say to the patient though.'

Nurse

'A lot of adults tend to have had other issues as well, earlier in life. A lot of them might have other mental health issues, so they'd quite often need antidepressants and seeing a psychologist, or if they're suicidal, seeing a psychiatrist.'

GP

Even if frontline workers believe an issue does have an online safety component, they find it difficult to know what to do with this information. As noted, workers have very clear guidelines about mandatory reporting (where a child is in danger) and can have strong protocols for family violence e.g. for maternal and child health services. However, the pathways are less clear for online safety incidents. Managing incidents well is made more difficult because

workers don't have good information about what they could or should be doing.

'It's not really clear cut what to do in that situation. You couldn't pass on their names to anyone unless they asked you to. There is no mandatory reporting of abuse when it comes to adults. It's up to them, whether or not they want to seek help. I wouldn't know where to go to get resources.'

Allied health worker

'You're always treading a very fine line with people who are vulnerable, complex and traumatised, because you want to maintain [the] therapeutic relationship. If I had gone to the police on her behalf and reported this, it may have damaged our therapeutic relationship, which may not have resulted in her going into accommodation, which was the most important thing. I think I probably still couldn't have done much differently. I would probably ... Yeah, I don't know what I'd do differently.'

Allied health worker

4. Some key terms are not understood

Key terms used in this study including 'image-based abuse' and 'technology-facilitated abuse' are not intuitively understood by frontline workers. Some aren't even sure what 'online safety' is. Other terms like 'sexting' are understood by people who work with teens, but unfamiliar to others. Frontline workers do understand terms used in the media like 'cyberbullying', 'revenge porn' and 'cyberstalking'.

'Okay, can you clarify again, just to make sure I'm [on] the right page like you, when you say online issues? What does that mean?'

GP

Despite all the barriers to online safety incident prevention and management, most frontline workers became more interested in the issue during the research interviews.

They indicated demand for setting-specific training and resources that tailor information for different groups. Frontline workers do not believe that resources developed for other professions will be relevant to them and are reluctant to devote time to adapt generic resources. This could be addressed by developing resources with frontline workers, or with their training, registration and professional bodies. This is expected to lead to greater engagement, increased relevance and to reduce the challenge of engaging these workers, making both easier – and hence more likely.

To the extent that it exists, and noted above, frontline workers' knowledge of online safety and how to address issues has been built through their personal knowledge/experience as parents and users of technology. It has also been built through trial and error through responding to incidents raised in their workplaces – rather than systematic training and resourcing. This shows that there is a need to better establish frontline workers' professional knowledge and resources.

Some settings are more likely than others to act in response to an online safety issue. Frontline workers who see their remit as being 'the whole person' appear more likely to see online safety as part of their role. Educators, more than health professionals, are more alert to online safety risks for children and young people and are more used to seeing incident prevention and management to be a part of their role. The necessity to act on an online safety issue is more clearly defined for older children and young people than it is for very young children or adults.

A variety of resources are being used in primary and secondary school (including those from eSafety), although educators note there is a gap in resources that teens consider credible. That said, many frontline workers don't necessarily know resources exist or where to find them. In early childhood and health settings, resources aren't being accessed at all.³

³ Note that this research was conducted in 2019, prior to the release of eSafety's Early Years Program. esafety.gov.au/about-us/what-we-do/our-programs/esafety-early-years-program

Barriers in dealing with engagement

This section provides an analysis of the behavioural and broader environmental changes needed for frontline workers to engage more extensively with online safety incident prevention and management, using the Michie COM-B model.⁴ This analysis model considers ‘Capability, Opportunity, Motivation + Behaviour’.

1. Capability: knowledge and skills

As noted, frontline workers’ capacity to deal with online safety issues is shaped by their personal knowledge and experience. Knowledge of online safety issues and how to address them has been built through personal knowledge, experience and trial and error, rather than professional training and resourcing. At some schools, online safety prevention is addressed as a matter of course, but this is the exception. The larger need is to integrate online safety into professional development and the curriculum.

2. Opportunity: a conducive environment

In most cases the prevention, and management, of online safety incidents is not part of frontline workers’ responsibilities and there is no established standard for professional development or action.

This is because most online safety risks and incidents occur outside frontline workers’ work environment, affecting their ability and incentive to act. The exceptions to this are secondary schools where educators can observe young people using internet-enabled devices, youth workers who oversee their clients in group homes and law enforcement, where family violence is seen as an important responsibility.

Outside mandatory reporting and referral pathways for victim-survivors and perpetrators in law enforcement, there are no clear pathways or support systems for addressing online safety incidents.

⁴ Michie et al (2011). ‘The behaviour change wheel: A new method for characterising and designing behaviour change interventions’. *Implementation Science*, 6: 42.

Frontline worker settings appear to have rich opportunities to intervene in online safety. For example:

- Because of the potential for deep personal relationships between early childhood educators and families, they are in an ideal position to intervene at a holistic level to support families and children to be safe online.
- Primary school educators also have close personal relationships with the children in their home room, and secondary school educators in wellbeing and student coordination roles have a pastoral care role. These workers can be encouraged and equipped to undertake preventative work and intervene if incidents occur.
- Secondary school educators responsible for relevant subjects such as IT and legal studies can weave digital citizenship into their curriculum.
- Health professionals, including psychologists, sexual and maternal health nurses, child health nurses, and GPs are well placed to observe the impacts on people who have experienced online safety incidents, even if they are not alert to them.
- Law enforcement workers are primed to act, however, they need referral pathways where their response is limited and more practical education, resources and supports in other cases. In addition, issues such as uncertainty about how to capture online/social media evidence and difficulties accessing information from social media or telecommunications companies need to be addressed for these workers to act.

3. Motivation: conscious inclination and unconscious bias

Most participants in the research felt a strong duty of care toward the wellbeing of their students, patients and clients. However, this didn't always extend to online safety.

Encouraging professional bodies to develop policies and guidelines, as well as providing easy ways to insert online safety into existing practice, could trigger engagement for those who don't have a natural motivation.

The research also found that a crucial aspect to address is workers' low sense of efficacy. Frontline workers need to feel better equipped to act and that their intervention will make a difference.

Support needs

Frontline workers identified several knowledge/skills gaps which, if addressed, would support increased engagement, with training and resources specific to each setting. These include:

- A map of the online environment: risks, signs of impacts, resources, supports and referrals to manage incidents. This would ideally be a one-page ‘cheat sheet’ rather than expecting professionals to spend time reading a very detailed document or set of knowledge.
- A guide to prevention, where preventing incidents is perceived to be part of their role by workers, such as youth workers, maternal and child health nurses.
- Practical health pathways, as relevant to individual settings, to guide action – and reflecting the clinical evidence.
- Investigation cheat sheets to support law enforcement professionals.
- A decision process to help frontline workers guide students, patients and clients to further support.
- Resources that can be provided by frontline workers to students, patients, clients and their parents.
- Guidance for frontline workers about how to have difficult conversations with their client or their parent.

Greater online safety knowledge means that frontline workers will be better equipped to act by having an increased awareness of the real risk of incidents – and knowing the benefits of acting. This will help minimise harm by ensuring the frontline workers are able to pick up on issues more easily and set their clients on the path to the assistance that they need.

Conclusion

Frontline workers face a number of systemic barriers which may mean that they are not well equipped or positioned to deal with the online safety issues of their clients.

One valuable solution is to increase frontline workers' knowledge of online safety issues which will better equip them to take action. It will also help them to see that online safety incidents are likely to happen and there are real benefits to taking action. In addition to equipping individuals to act, normalising action – which could be signalled by professional bodies, employers and highly visible champions – is important.

There are valuable opportunities to raise awareness among frontline workers and a clear need for highly targeted resources to be developed, tailored to specific settings and cohorts.

There also appears to be a large advocacy opportunity, working with training organisations, peak and registration bodies, as well as state, territory and federal government funders and regulators (such as health and education departments) to better integrate the online/digital world into frontline workers' professional practice. Training, resourcing and practice to a large extent reflects a pre-digital world when it comes to supporting health and wellbeing: education, health and law enforcement sectors now need to evolve in order to truly reflect the world today.

eSafety has used these findings to inform ongoing work to support frontline workers and peak bodies, including frontline worker training and outreach presentations.⁵ It also supports eSafety's interactions with police, educators and counsellors on cyberbullying and image-based abuse complaints.

The research formed part of the evidence base underpinning our [Early Years program](#),⁶ including professional learning modules and resources. This launched in January 2020. It was also used for eSafety's [Toolkit for Schools](#), launched in February 2020. The Toolkit supports a nationally consistent approach to

⁵ [esafety.gov.au/key-issues/tailored-advice/frontline-workers-support-providers](https://www.esafety.gov.au/key-issues/tailored-advice/frontline-workers-support-providers)

⁶ [esafety.gov.au/about-us/what-we-do/our-programs/esafety-early-years-program](https://www.esafety.gov.au/about-us/what-we-do/our-programs/esafety-early-years-program)

preventing and responding to online safety issues and was developed in collaboration with the education sector.⁷

⁷ esafety.gov.au/educators/toolkit-schools

Methodology

Cohort descriptor	Other sampling criteria
Early childhood educators and carers (n=15 interviews)	<ul style="list-style-type: none"> • Experience working with preschool children (aged 0 to 5). • Range of digital literacy. • Range of early childhood education settings, i.e. preschools/kindergartens, long day care and family day care. • Minimum of 4 x with experience teaching children with a culturally diverse background.
Primary and secondary school educators (n= 15 interviews)	<ul style="list-style-type: none"> • Educators were recruited as having experience in either: supporting a student through an online safety issue or (If they taught prep-year 2) having exposure to online safety issues within their working environment to an extent that they could comment on students' experiences of online safety or technology use • Quotas were set to reflect: <ul style="list-style-type: none"> ○ school sector i.e.: 5 x Government, 5 x Independent, 5 x Catholic schools ○ gender (roughly 50:50 split overall, although the primary school sector was skewed female) ○ roles and responsibilities within the school i.e. mix of: wellbeing leaders/counsellors, year level coordinators, general classroom educators, specialist educators, year level educators, with and without pastoral care responsibilities ○ 3 x Prep-Year 2, 3 x Years 3–4, 3 x Years 5–8, 3 x Years 9–10, 3 x Years 11–12.
General practitioners x 8 Allied health professionals x 10	<p>All GPs and allied health professionals had either:</p> <ul style="list-style-type: none"> • experience in treating a patient or client of any age who has experienced an online safety issue such as cyberbullying, image-based abuse or technology-facilitated abuse in situations of domestic or family violence, or • exposure to online safety issues within their working environment such that they could comment on patient/client experiences of online safety issues. <p>Quotas for allied health professionals were set to reflect:</p> <ul style="list-style-type: none"> • psychologists (x 3) • case workers and carers who work with children in out-of-home care (x 2) • maternal and child health nurses (x 2) • health professionals working in sexual health settings (x2).
Police officers x 16	<p>All participating police officers had experience directly interacting with an adult complainant regarding an online safety incident e.g. cyberbullying, image-based abuse or technology-facilitated abuse in the context of domestic violence (no child complainants).</p>

Cohort descriptor	Other sampling criteria
	<p>Quotas were set to reflect:</p> <ul style="list-style-type: none">• range in years of service (<10 years, 10 years+)• 8 x police officers in specialised units (sexual offences, electronic or computer-assisted crimes, domestic violence)• 8 x local police (front desk officers, based in local police stations).

