Transcript for Online Safety Webinar

[Welcome]

Hello and welcome to our Online Safety webinar. This webinar is two and a half hours long and we'll have two five-minute breaks within that time. You should have received a link to the PDF of the slides and the handbook for this course, you will need those throughout the discussion so please have them ready. There are accessible formats available, so please let the host or the co-host know if you would like those. Ideally, we would like your webcams enabled, but we ask that you keep microphones muted unless you are participating in a discussion or asking a question. We do this because we want to minimise the distractions that background noise could create for people, but we also want to be able to see that everyone is here and engaged. We understand there might be occasions when you would prefer to have the webcam off. For example, if you're having problems with your internet speed, or you've got children who need your attention.

Just to say that information shared can be of a sensitive nature, and some of the content is not appropriate for children, so if children are in the room, please consider using headphones and angling your screen away. Also, if you're happy

to share any of your own experiences, please bear in mind confidentiality. We ask that you anonymise any examples, experiences or stories that you share.

It is important to keep yourselves emotionally safe during the training and if you need to take a breather from the webinar, that's okay and you can rejoin whenever you feel able to. It might be good to think about somebody you could reach out to if uncomfortable feelings or memories come to the surface. You might need to find support for yourself, or it might be that you're concerned about someone else or another situation after the session. If that's the case, please do contact our help-centre as soon as you can because the trainer is not equipped to give specific advice on the webinar platform.

The chat facility can be used throughout for questions and for participation in activities. The co-host might answer the question, signpost you to further sources, or hold on to that question for the next pause and share it with the host. If a question is not answered, or a question is about a very specific issue, please do contact our safeguarding help-centre by email or phone.

Thank you for choosing Thirtyone:eight for your training today. Our motivation is to equip, empower and encourage you in your safeguarding responsibilities. As we start, we just want to recognise the time, care and commitment you're investing in your church, charity or organisation by attending this training and in

everything that you do, thank you. I hope that the message you get today is that you never have to do safeguarding alone. As I mentioned already, we have a help-centre; you may want to pop contact details into your phone now if you don’t already have them to hand. The help-centre is there to support you with any questions regarding safeguarding. It might be queries about policy, or you might have a live situation which you'd value talking over with us and getting advice. The helpline operates from 7am till midnight, seven days a week, 365 days a year, or 9am to 5pm Monday to Friday for those regular questions about policies, guidance and processes, and the out of hours service for any more immediate concerns.

Everyone here today will have a different motivation for engaging with safeguarding. For us at Thirtyone:eight, it comes from our passionate belief that safeguarding is close to God's heart. Our name comes from a verse in the Bible, Proverbs 31:8 that says, “Speak out on behalf of the voiceless and for the rights of all who are vulnerable.” When we take care of the vulnerable, we are fulfilling God's call. If you're part of another faith group, you may well recognise this call from your own sacred scripts. Or you might be part of a charity that has care and dignity for the vulnerable at its heart. Whatever your motivation, we want to equip you.

[Introduction]

The online world is evolving quickly, with new things happening on a daily basis. Trying to keep up with changes can seem overwhelming. The aim of our course is not to tell you about every new thing that's happening. It wouldn't be helpful, and we'd have to write a new course each week! There are lots of links in the handbook to resources which will help keep you updated with the latest developments. The ‘signposting’ section can be found towards the end, and there are also appendices on various topics such as basic cybersecurity and support for parents and carers.

The quote on your screen is part of a longer one that states: “Against a backdrop of a sharp rise in online hate, the spread of disinformation, and an increase in online fraud and scams, organisations face the ongoing challenge of finding ways to protect their communities online… When you consider the fact that charity communities often include vulnerable or at-risk members, online safety must be at the heart of community management.” That quote comes from Charity Comms, UK and there is a link to it in your handbook. It emphasises that, actually, we have to have online safety as part of how we work with our communities to ensure they're safe and that we are doing everything we can to recognise the risks that people face, but also protect them from risks that we might inadvertently expose them to.

So, how does online safety fit into the wider world of safeguarding? You can see on your screen physical, emotional, neglect, sexual and financial abuse – forms of harm recognised in safeguarding legislation throughout the UK. In this course, we will be using a safeguarding lens to view the world of online safety.

What does this mean? Well, firstly, we need to recognise that online forms of harm and abuse are as real and important as those that take place in the physical world. This is reflected in the fact that online harms are named in safeguarding legislation and guidance across all 4 nations of the UK (your handbook has information on some of the relevant laws and national guidance). In 2023 there was the introduction of the Online Safety Act, which covers the whole of the UK. This law mainly gives duties to tech platforms and companies, but its creation shows how important this area of safeguarding is and recognises the potential for serious harm that can occur online.

As charities, churches, and community groups, our safeguarding responsibilities include preventing and protecting people from harm that may come from within our organisation (from our staff, volunteers, activities etc.) and also responding to and reporting harm and abuse that those in our communities may be experiencing outside our organisation. In terms of online safety, this means having policies and procedures to make our own online environment and interactions as safe as possible and also having an awareness of what online

harms people may be experiencing in their own lives and how to respond well if we think this is happening.

This is a non-technical safeguarding course. We won't be exploring all the security settings on different apps (there is signposting in your handbook to resources that can help with that). Instead, we will help you ensure that your organisation is equipped to incorporate online safety into your safeguarding practice. We will raise awareness of various issues, consider some case studies, and give you time to reflect upon your own organisation and the areas of potential safeguarding risks and ways to reduce them.

So, let's pause and consider, what would be a good outcome for you today? What's brought you here? What's your role? What are you hoping to gain from this course? Please just put your thoughts into the chat, or feel free to unmute at this point and or raise your hand, and we'll have a few points from you. So, what's brought you here? What's your role, and what are you hoping to gain from this course?

The online world is a significant environment for all people of all ages in the UK. Here are just a few statistics to illustrate why online safety is something that we all need to consider: 25% of three- to four-year-olds now have their own mobile phone, according to Ofcom data of media uses in 2024. 61% of 16- to 17-year-

olds have experienced something nasty or hurtful online or know someone who has. In an Age UK survey at the end of 2022, 66% of adults aged 75 and over had used the internet in the last three months, which was up from 29% a decade earlier. And UK adults spend an average of three hours and 41 minutes online every day. With such widespread internet usage in our UK environment, we need to take online safety seriously.

Across the UK, online safety is included in national legislation and guidance for education and child protection. Our training is split into four modules, each focusing on a different area of online safety identified as the 4 ‘C’s. The original four C's were developed by Livingstone and Stoilova as part of a Europe-wide project on online research and evidence but they have been incorporated into guidance from many UK-wide organisations and into some national policy and guidance too.

These four ‘C's help us to look at the various key areas of risk, the responsibilities we have and the risk reduction measures we may be able to put in place.

The Four ‘C's are:

Content - that's videos, words or images posted online that may be illegal or harmful.

Contact - that's harmful or inappropriate interaction with others.

Conduct - harmful ways that people can behave online, and

Commerce - harm through scams, phishing or other financial risks. This is sometimes referred to as ‘contract’.

In each module, we will identify some of the potential risks, recognise what our responsibilities are, and explore how we can reduce the risk of harm in our communities. Your handbook contains a mini audit tool to accompany the session so you can assess how you're doing in each area and build an action plan to make your organisation safer.

[Module 1: Content]

So, let's start with ‘content’ in module one.

In this module, we will identify some different types of harmful content and the impact they can have. We'll explore how we can reduce the safeguarding risks for vulnerable groups in our communities and recognise our safeguarding responsibilities in this area.

So, let's pause and consider once again. What harmful content are you aware of?

Feel free to pop your thoughts into the chat or again, raise your hand and unmute. It'd be lovely to hear from you some of the different things that you may be aware of regarding content that might be harmful to anybody who's accessing the online world.

Some examples could be - abuse images; content that incites violence, self-harm or suicide; content that's inciting hatred or extremist views and radicalisation; it could be racist, misogynistic, ableist and homophobic viewpoints and other types of discrimination. It might be techniques and creation of weaponry for terrorism. Perhaps 'deep fakes' - a digitally manipulated image or video to make someone look or sound like somebody else. Pornography is a big issue, particularly when illegal or viewed by children. And we have violent content; content that promotes disordered eating; artificial intelligence; gambling websites. There's a myriad of material out there that could potentially be harmful, and a lot of it is very easily accessed.

So, let's look in more detail at some of this content. When we start to look at the dangers related to the content on the internet it would be overwhelming to consider every aspect of potential risk. We are going to highlight a few areas that will hopefully provide you with some awareness of the safeguarding risks and then consider how we may help others prevent access to that harmful content. As we discuss these, think about how these relate to the forms of harm and

abuse named in legislation. There is a wealth of further information in your handbook that covers some of the other areas.

First, let's consider abuse images. In 2023, the Internet Watch Foundation received almost 400,000 reports of websites hosting child abuse images. Each website could represent anything between one and thousands of images. In turn, each image represents a child who has been harmed, and potentially many others too.

Secondly, pornography. Adult pornography is mainly legal in the UK, but indecent images of children are not. Views differ as to whether legal adult online pornography is harmful, but there are safeguarding implications to consider, particularly around the normalisation of sexual violence, the ease with which children can be exposed to pornography online, and the links with modern slavery and trafficking. There's more information in appendix seven of your handbook around this issue.

The third issue we'll consider is artificial intelligence, or AI. AI is best defined as being computer systems that are designed to act in a more human way in order to undertake tasks normally reliant on human intelligence. These systems are able to analyse data and make predictions about potential next steps. They are able to learn from mistakes and change how they approach to future tasks.

AI is a source of much speculation at the moment. It has many benefits – it can make tasks easier and opens up opportunities for creativity and scientific discovery. However, there are also safeguarding concerns around it. One of the major concerns is its ability to generate very realistic fake texts, images and videos.

In 2023, the Internet Watch Foundation (IWF) investigated its first reports of child sexual abuse material generated by AI. Their report states:

“Initial investigations uncovered a world of text-to-image technology. In short, you type in what you want to see in online generators and the software generates the image…These AI images can be so convincing that they are indistinguishable from real images.”

Another report states:

“Malfunctioning or maliciously used general-purpose AI can also cause harm, for instance through biased decisions in high-stakes settings or through scams, fake media, or privacy violations.” International Scientific Report on the Safety of Advanced AI. There is more information about AI in Appendix 2 of your handbook and the following quote illustrates powerfully the harm that false images can inflict.

“My whole body was hot and I just let out a scream…” This quote comes from Jodie – a victim of image theft and deepfake pornography, speaking on BBC File on 4 “Degraded by Deepfakes” released in April 2024. Jodie was confronted with photos and a video showing her having sex with a number of different men. It’s hardcore pornography, with her face photoshopped on. It’s all fake, but some of it looks real. She goes on to say: "This is affecting thousands of women. People are taking their photos without consent and doing whatever they want to them…we need to have the proper laws and tools in place to stop people from doing this."

Sexually explicit deepfakes are now illegal in UK law (the Online Safety Act covers the sharing of these images and videos and updates to the Criminal Justice Act announced in April 2024 cover the creation of them).

Whilst the internet contains a vast amount of helpful information and the ability to entertain, it also has the capability of spreading harmful and hateful material and ideologies. Exposure to these is a safeguarding concern – think back to that initial slide about physical, emotional, neglect and sexual abuse and you will see how these forms of harm can be present here.

First, self-harm and suicide, including the ideation of these. Poor mental health is on the increase across the UK and many people seek guidance and support from

the internet. Unfortunately, there are some harmful websites that advocate self-harm as a coping strategy. There are also some sites that promote suicide. People can use social media to develop their own sense of self-worth. This is easily exploited by people intent on harm. Molly Russell died by suicide in 2017 after engaging in discussions online about her worsening depression, she had accessed 1000s of images and articles concerning suicide and self-harm. She also had a secret Twitter account that she used to express her thoughts and discuss views with other individuals.

There are also many sources of violence online. Content accessible via the dark web and more openly available platforms far exceeds what people may view on TV and in films. Brianna Ghey was murdered in February 2023 by two teenage children. The violent attack was meticulously planned via messaging apps and drew upon the fantasy violence that they had been viewing. There's a detailed report you may wish to listen to that the co-host can link to in the chat. If you choose to access this, please do so with care as it could be very upsetting.

We're going to go into breakout rooms now, and we're going to give you a chance to have a discussion and think about how we might reduce some of that risk relating to online content. So, your discussion question is: ‘How can we reduce the risks posed by harmful content?’ We're going to have seven minutes to discuss this. After six minutes, you will get a one-minute countdown timer, just

for you to know that it's time to start wrapping up your conversation. Please nominate someone to share feedback so that when we come back to the main group, you'll be able to just share some of the thoughts from your discussion.

OK, I hope you had good discussions. Let's get some ideas. It may be raising awareness within groups in an age-appropriate way. The UK Safer Internet Centre has Safer Internet Day every year with free resources that are organised by age group, from three upwards. Having open conversations is also a good idea. This can normalise talking about issues, reduce any misplaced sense of shame and offer hope to anyone who feels overwhelmed. You could sign up to information sites and newsletters or apps such as the National Online Safety app, or Scotland's Parents Club, to get updates and ideas of what you can do to support people in your community. There're lots of options for you to explore in the signposting section towards the back of your handbook.

Other ideas include having safe / acceptable usage policies for staff and volunteers; using filtering and parental controls to restrict what can be accessed within your setting, and maybe promote these to families related to your community so they can be used at home. Stick to the age restrictions for social media and messaging sites. There are guides available online, again, accessible through our handbook, that will help you discern which social media platforms can be used safely for specific ages – that's a really a useful guide to signpost

parents to. Consider how, where and when vulnerable groups might access the internet. Are children’s phones allowed in rooms on residential trips, for instance?

Consider using accountability software if you're supporting someone recovering from addiction to harmful content. There are some fantastic resources out there for those people who are struggling with addiction to harmful content, such as pornography or indecent images, and accountability software can be used to support them.

So, to finish this first module, we're going to take a look at our mini audit that is in your handbook, on pages six to seven. Let's consider how we can fulfill our safeguarding responsibilities in terms of online content. The mini audit tool in your handbook will help you do this. Just spend a few minutes looking at this and asking any questions, if you have them. This tool is something that you're going to be able to use as you go away from this course. Don’t feel you have to fill this audit in in-depth now, you might want to pop some thoughts down on it as we go, but what I really want you to do is just clarify you understand those questions. If there's any area that you're not quite sure of, please use this opportunity to ask.

Here are some of the key things to remember in terms of fulfilling our responsibilities in relation to online content. Firstly, and as always, tell your safeguarding lead if you're concerned that someone in your community has seen

or experienced harmful content. We also need to have clear policies and procedures about what content can and cannot be accessed on your organisation's devices, shared with vulnerable groups and posted on your website, or social media site, so people are aware of those boundaries. Your policy should also detail what people should do if they find harmful content. Safe usage agreements should be in place for staff and volunteers. You can use filters and strong passwords to protect your organisation's devices and WiFi networks. Who has permission to update your website and social media? Ensure they have clear codes of conduct and access to the correct training around safe content. You need a clear policy and risk assessment for live streaming and using photographs, including parental consent and not sharing children's names alongside their photos. For some children, it will never be safe for their photos to appear online.

Thirtyone:eight members can access our sample online safety policy, alongside many other sample policies, forms and resources, in the Knowledge Hub section of our website. NSPCC also have a free template policy available for any organisations working with children.

[Break 1]

We're going to go into a break now, and you're going to have just five minutes. It's not very long. Please just turn your camera off but don't leave the Zoom meeting. There's a countdown timer on the screen for you. I'll see you in five minutes.

[Module 2 – Contact]

Welcome back. It's amazing how quickly five minutes goes when you're trying to get a cup of tea, isn't it?! Good to see you all back. We're going to go into Module Two now and think about online contact.

In this module, we will consider the different ways in which we can contact each other online and the risks involved. We will look at the importance of accountability and transparency in maintaining safe contact in our communities, and we will recognise our organisation's responsibilities to reduce the risk of harm through online contact.

One of the biggest risks of the global connections that the internet enables is the easy anonymous access that perpetrators can have to vulnerable groups. This risk is exacerbated by the fact that contact can happen in environments where vulnerable people feel physically safe, so they may not be so alert to danger, and their carers may be unaware of what is happening.

The quote on your screen comes from a report into online sexual harm of young children by Susie Hargreaves, OBE, the chief executive of the Internet Watch Foundation, and she said: “The opportunistic criminals who want to manipulate your children into disturbing acts of sexual abuse are not a distant threat, they're trying to talk to them now on phones and devices you can find in any family home.” It’s a sobering thought.

So, let’s come back from that stark warning to a gentler place and just pause and consider what online contact there is within your community. Think about your context. Who do you contact online in your role? What other online connections are there in your community? Feel free to pop your thoughts into the chat, or just wave your hand and unmute and we'll hear some verbally as well. You might have contact with friends, with team members, colleagues and leadership within your organisation. You may communicate with parents connected with youth and children’s work. Do you contact any vulnerable groups? Do you contact the public or wider community?

Online connections can include email, messaging services, group chats, social media. Also Zoom or other video call platforms, which can be used in a one-to-one situation or a group situation, like we're in today.

We're going to consider a case study now around the issue of online contact.

We're going to do this all together, and our co-host, will kindly read the scenario so that we all have access to it. It's also in your handbook if you want to follow along that way too. Have in mind the following questions: what are the risks in this particular situation, and what are your safeguarding responsibilities?

Rachael is 37 and is a volunteer youth leader for your organisation. Her own children are in the preschool group, and she and her family have been members of your community for a number of years. She's a popular leader, and lots of young people look up to her and ask her for advice about friendships, school, etc. She's accepted a couple of social media requests from young people in the group, and recently, one of the girls started to message her privately after getting her number from the youth WhatsApp group. They've been messaging daily, often in the evening, about difficult relationships the girl has been having at school. The girl's parents have raised a concern, because they have found out about this.

So, what are the risks in this situation? What are your safeguarding responsibilities?

Our primary concern is that the girl's safety and wellbeing might be at risk. Could Rachael be using her position of trust to groom? Even if not, she’s modeling

unsafe behaviour by normalising children and adults messaging privately- this could put the girl at risk of harm from others.

Thinking about it from another perspective, Rachael is open to an allegation in this situation. One-to-one messaging online is like being in a room alone with someone with the door closed. This isn't safe working practice, and we need to help our staff and volunteers recognise their responsibilities in the online environment as well as our physical spaces.

This unsafe contact could damage relationships within your community too. What is the girl's perception of her relationship with Rachael? Rachael may have one view of what this communication means, and the girl may have another. Without clear, healthy boundaries this can easily happen. How will the girl's parents respond to Rachael and your organisation? This situation could break trust or even put Rachael at risk. If there is unsafe contact in your organisation, what does this communicate to young people, other volunteers, parents, etc? What precedent does it set? There is a risk to the organisation's reputation as well.

So, what are your safeguarding responsibilities? First of all, we are going to respond well. We might thank the girl's parents for talking to us and confirm that we will pass on their concern. We wouldn't minimise or excuse Rachael's actions. You need to tell your safeguarding lead so they can take the appropriate

action and record it. If you are the safeguarding lead, check your records for any existing concerns about Rachael or the girl. Assess risk and follow your next safeguarding steps (which will vary depending on this risk assessment). Appendix 5 is an online safety flowchart that may help you discern appropriate actions. Talk to our helpline for advice if you need it.

We might review the code of conduct for youth leaders. Has Rachael contravened clear guideline, or were expectations unclear? We may need to update that to ensure it doesn't happen again. Ensure all youth leaders have a clear code of conduct that includes expectations about safe communication with young people.

As with any safeguarding concern, don't approach the girl or investigate anything yourself. As mentioned earlier, the safeguarding lead will check records for any existing concerns about Rachael or the girl and take the next steps in the safeguarding process. Ensure that Rachael has appropriate supervision and support.

Thank you for your feedback, we hope you found working through that scenario helpful. We're now going to think more widely about the potential safeguarding risks when contacting vulnerable groups online and the steps we can take to reduce them.

Any online contact has a number of potential safeguarding risks, including unsafe sharing and use of personal data, including GDPR infringement and a lack of transparency and accountability. Our policies should help us to account for and reduce these risks. When we are working with vulnerable groups, we have some additional safeguarding risks that we might need to be aware of.

Our organisations have safeguarding responsibilities towards children and young people. Children are vulnerable because of their age, their relative lack of experience, and their reliance on adults. Because online contact is easy and anonymous, those who seek to groom children may use the access provided by an online platform to build trust and develop a relationship with a child in order to perpetrate harm. Children might also be enticed to share personal information that can then be used to gain further access.

A lack of clear, safe boundaries in online contact with children and young people can be a safeguarding risk. There is the potential for unhealthy attachments, hurt and misunderstanding through unrealistic expectations and the modeling of unsafe behaviour - if a trustworthy adult is messaging me online, one-to-one contact with adults is probably fine.

If online contact involves groups of people, there is risk through our lack of control over the messages of others in the group. There's potential for

inappropriate content or conduct that could cause harm to children and young people.

Some apps and messaging services are only designed for those above a certain age. If children younger than that access these platforms, this is a safeguarding risk as they may be exposed to interactions that are not safe or age appropriate.

Some of the things we can do to reduce the safeguarding risks associated with online contact are to have a real clarity of purpose as an organisation in our communication.

When we're working children and young people, the ideal is to avoid online contact. If I was teaching a course about lifting things safely, I would be saying, "First of all, do you have to lift it? Could you avoid lifting it? Is there an alternative to that?" And that's a similar thought process to this: Is it actually necessary to contact these children online? What are the alternatives? What are the risks of not communicating in this way at this time?

If we are going to engage in online communication with children and young people, we will want to ensure that we have parental consent to do so, that we're not having one-to-one conversations, that contact involves at least two safely recruited adults for transparency and accountability. Contact should be within office hours, or an agreed period, so it's clearly part of your role in the

organisation - not a personal relationship. It is also important that contact is made via an organisational email address or messaging account. This is both for clarity and so that data can be included should it be needed in any investigations or subject access requests.

If we are messaging children and young people as part of a group, we need to restrict and monitor access to this group. The group should be monitored by at least two safely recruited adults. We would remove people who are no longer volunteering, for example, and young people who are no longer part of the group. We wouldn't have unchecked adults or other parents in a group with children. We would ensure that any adults in those groups would have been through a safer recruitment process, as we would for any volunteers working with children and young people in the physical world.

There should also be limited sharing of personal data. Think to yourself, if I was someone seeking to groom or cause harm, what information could I access via this group? Keep security settings high so data can’t be accessed easily and explore communication options with safety in mind. For example, WhatsApp Communities can be used so that group members can't see and use numbers, and replies are restricted.

For certain roles, and this will very much depend on your organisation and your size and needs, it might be that actually certain members of your staff or volunteers should have access to a work / organisation device so that any contact is done through that official phone, tablet or laptop. This gives a greater level of transparency and accountability and makes boundaries clearer. That's not going to be easy in a very small setting where you're relying on volunteers and you don't have the financial resources to supply such devices. If this is the case for you, then you need to think, well, how else are we being accountable? Who else is included in those conversations to ensure that we have accountability and transparency? For more considerations about safe contact with under-18s, see appendix three in your handbook.

If we are working with adults at risk of harm, there are many of the same safeguarding risks as for children and young people. Age restrictions aren't an issue, but capacity to give informed consent to be in a group might be. The accessibility of online communication should also be something that is considered.

So, to reduce risks, we need clarity of purpose in our communication. Again, is it actually necessary to contact this person online? What are the alternatives? What are the risks of not communicating? If communication is one-to-one, there needs to be clear boundaries and we need to build in ways to keep yourself

accountable and communication transparent. And again, contact should be within office hours.

As with children and young people, we want to restrict access to any groups that include adults at risk of harm. So, remove those who are no longer volunteering, or part of the group, or members of the group who move on. There needs to be a shared understanding and agreement of what the group chat is for and what it isn't for and how it's going to be used. It may be appropriate to ask people to sign that agreement.

There should be limited sharing of personal data, and again, we might consider if a work device is required by people in certain roles. That is the clearest way to separate personal and work communication. It also allows an additional layer of accountability and transparency as that device can be monitored to ensure that it is being used correctly.

On this next slide we will consider three forms that online contact can take, and the safeguarding risks associated with them: one-to-one messaging, group chats and public forums.

All of these forms of contact do have benefits. It's why we use them. This discussion isn't to stop you using them, but to do so intentionally, with awareness, and as safely as possible.

Firstly, one-to-one messaging. The risks are that it's harder to be accountable – this is a risk for our beneficiaries and vulnerable groups but also our staff and volunteers. Private messaging is open to abuse and allegation – like the analogy we used earlier of being alone with someone in a room with the door closed. There's also the potential for misunderstanding in written messages. Also, if messaging services are encrypted, they can't be easily monitored by security software.

To reduce these risks, we need to build in accountability processes and procedures if we are contacting vulnerable groups. We can establish clear boundaries and expectations. We could risk assess and consider our policy around encrypted messages – are there circumstances in which such services wouldn't be appropriate?

Our second form of contact is group chats. These can be really helpful for sharing information with a specific group in a quick and concise way. However, there are safeguarding risks through the sharing of personal data, intentionally and unintentionally, and there's reduced control for us as organisations over the content and the conduct within that group.

To reduce these risks, you can explore the privacy settings and controls available in the apps or messaging services you use. There is signposting towards the

back of your handbook to sites where you can find guidance about this. You could consider forms of messaging that limit data sharing and restrict participation. You could designate specific group administrators and ensure they've had the necessary training to communicate with the group safely and monitor interactions. Their code of conduct should include what to do if inappropriate content is shared or unsafe conduct occurs. Another way to reduce risk is to give clear guidelines to group users and ensure groups are limited to necessary people and for an agreed purpose.

Finally, public forums- for example an organisation's social media page or website. The safeguarding risks associated with these public spaces are mainly via access to personal details, photos and other sensitive data. There's also the public perception and reputation of our organisation to consider.

In order to reduce the risks, we can ensure that we restrict who administrates our own websites or our organisation's social media pages, and ensure that the people who do this are trained and given clear guidance, including what to do if they have any concerns.

We can build in accountability and support for them too. We can be intentional in setting permissions, filters, etc. on our websites and social media platforms so that security settings are as strong as possible.

Be mindful when sharing images and videos, particularly of children and adults at risk of harm. Many people will now take photographs of people from the back when they're doing activities, so you can't easily identify people, but even then, we should still be open and transparent and seek permission to ensure that we are keeping everybody safe.

So, let’s finish this second module reflecting on our safeguarding responsibilities in terms of online contact.

In our audit on page seven, you will see a few considerations. For many of us, contact is the area of highest safeguarding risk for our organisation’s activities. We want to avoid inadvertently facilitating harm so let’s consider our responsibilities. Look at the contact section of your audit and ask any questions you have.

As always, tell your safeguarding lead about any inappropriate or unsafe contact, including where there's a potential for risk - we want to act before harm occurs. Have clear policies and procedures about: contacting vulnerable groups, the safe storage, sharing and use of personal data, and the management of social media groups.

Risk assess any online activities that you're facilitating and take steps to reduce risk. Provide training, support and accountability for all staff and volunteers.

[Break 2]

Well done. We're going to have our second break now. Again, just take five minutes to get a drink and have a comfort break. Please turn your cameras off and mute your microphones. We'll come back in five minutes.

[Module 3 – Conduct]

Welcome back. Our third module is about safe conduct. Conduct covers the way we and others behave in our online interactions. In this module, we will consider when online conduct becomes a safeguarding concern, identify some particular forms of harmful conduct to be aware of, explore the risks posed by harmful online conduct, and recognise our safeguarding responsibilities in ensuring safe conduct within our organisations.

So, let's pause and consider, what types of harmful online conduct are you aware of? Please feel free to pop your thoughts in the chat, or, as we've been doing, unmute and share your thoughts.

Some of the answers that we've had include grooming - using the access that's given by online contact to manipulate someone with the intent to abuse, often easily done by using a hidden identity. There is also coerced online child sexual abuse, children being groomed and coerced into taking indecent images or videos of themselves.

Cyberbullying is where bullying behaviors take place online. This may be in the way someone comments on a person's statuses, photos and messages posted on social media, or it can be direct emails and direct messages or posts about that person. It might be what's termed ‘pile on’ harassment - when a group organises to target an individual. It may be the use of offensive language or hate speech,

It could involve unwanted sexual contact. You may have heard the term ‘cyber flashing’. The UK Safer Internet Centre states that 76% of girls between 12 and 18 have been sent unsolicited nude images of boys and men.

It might be inciting violence.

It might be spreading misinformation to manipulate people’s views or actions, or manipulating someone into giving personal information. It could involve promoting or inciting self-harm, disordered eating and suicide.

There are dangerous dares and challenges that have unfortunately led to serious harm and death. You may have heard of the cases of Archie Battersbee and Isaac Kenevan who died after taking part in online pranks and challenges.

There is also gambling. Gambling is legal for adults in the UK, but it can become a safeguarding concern when it becomes addictive and harmful, leading to

emotional harm or self-neglect, or when it affects the safety and wellbeing of a child or adult at risk of harm through financial harm, or neglect, for example.

We're going to look at another case study together now, and this is about Harper,

As you listen to Harper's situation, think about- what are your concerns? And what are your safeguarding responsibilities?

"It's the first evening of your summer camp, one of the young people comes to talk to you. Harper is 13 years old and is quite shy and quiet. When you ask how they're doing Harper starts crying and explains, "The night before camp I was at a party. I've got some older friends - they gave me alcohol. It's the first time I tried it. I thought it was fun but now there's videos of me doing really, really embarrassing things all over social media. It's so shameful. At school they told us, 'Once it's online it's there forever' so that's it for me now. There're already loads of comments. All my friends will see, my family – I'll be in so much trouble. I just can't face it."

So, what are your concerns and what are your safeguarding responsibilities?

One of our primary concerns is for Harper's safety. Some of the language used is worrying. "That's it for me now", "I just can't face it." Young people can feel trapped and helpless at the prospect of things they don't want public appearing online. 16-year-old Murray Dowie from Dunblane took his own life after a

sextortion scam. He was tricked into sending intimate pictures of himself to someone he thought was a girl of his age. The perpetrator then pressured him for bank details with the threat of sending the photos to all of Murray's contacts if he refused.

In Harper's situation, we don't know what the videos show. Harper said, "It's really embarrassing and shameful", and that could mean many things. Are these abuse images?

What are the comments? Are they abusive? Is this cyberbullying?

We would also be considering if there are any concerns known about Harper's family? Does "so much trouble" mean Harper's at risk of further harm?

Then we might also have concerns about Harper's wider wellbeing. Who are these older friends? Why are they giving Harper alcohol? Is there a risk of exploitation? Are the videos for control or blackmail?

So, let's move on to our safeguarding responsibilities. First of all, we are going to respond well to Harper in this moment. Thank Harper for talking to us. Reassure them it was right thing to do, listen well, affirm and value.

Next, report or refer. Talk to your safeguarding lead straight away. You can call our helpline if your safeguarding lead isn't available at this time. If you are the

safeguarding lead, you can call our helpline for advice if you need it and refer to statutory agencies or other bodies as necessary. We know many of our members have our details in your safeguarding policies, so it's easy to find and use us, but please make a note of our helpline number in your handbook as well.

Follow their advice about steps to ensure Harper's immediate safety and subsequent support. You or your safeguarding lead could ask some clarifying, not leading, questions - TED questions (tell, explain, describe), which give the opportunity for Harper to explain more without us leading the conversation, to find out more about what videos and comments are and what they involve.

The safeguarding lead would report this externally as necessary i.e. to the police if a crime has been committed, CEOP (Child Exploitation and Online Protection command), perhaps social care services.

If the videos are nude or sexualised images, Childline have a ‘Report-Remove’ tool that can have them taken down. Whatever you do, don't ask to see those videos yourself. Harper might want to show you and say, “look how embarrassing it is”. You do not want to see it. There may be some illegal, illicit, indecent images on the video. You do not want to see it, you would be viewing indecent images of a child, which is against the law, but you're also exposing yourself to seeing something that you really do not want to see.

There are lots of organisations that may be able to help Harper and give them expert advice and help. Lots of these are listed in the signposting section of your handbook.

Something we can do going into the future might be to talk to vulnerable groups in your organisation about how to keep themselves safe online, including what to do if they do something they regret, so it normalises the experience and offers hope.

Ensuring that Harper knows there is hope is vital. Our use of our language when responding to safeguarding concerns is very important. The phrase used in the scenario “once it's online, it’s there for is there forever” can be soul destroying for someone who's been tricked into sharing explicit photographs. There are tools available to remove and assist people in these situations, and it's important that we instill a sense of hope, not fear. This quote is from Jim Gamble, former head of CEOP: "Too many people tell children ‘what goes online stays online’…That takes away hope and hope is what fuels children through these difficult times." "The key is the sooner you talk to a trusted adult, the sooner something positive can be done and I'm telling you from years of experience in this field, things can be done.”

Moving on from that scenario, we're now going to identify some specific safeguarding risks for our organisations associated with unsafe online conduct.

The primary safeguarding risk of unsafe online conduct is harm to vulnerable groups. I'm sure you can all think of stories you have heard in the news or from your own lives where somebody's behaviour online has caused serious harm to another person. The anonymity of the online environment means people can sometimes behave in ways that they would not consider doing in the physical world, and for those who intend to cause harm, online platforms offer an extra layer of secrecy and security - and abuse thrives in secret. As organisations, we have a duty to ensure that our staff and volunteers behave in safe ways online so that no vulnerable groups are harmed through interaction with our activities.

We also need to ensure staff and volunteers are aware of what's expected of them in terms of online behaviour, what is acceptable and what isn't? Does our organisation have expectations about how someone conducts themselves on their personal social media? We need to ensure people are fully informed so they aren't leaving themselves open to an allegation or loss of position without realising it.

Unsafe conduct of staff and volunteers, or others in our community, in online groups, can lead to reputational damage. Protection of our reputation is never the

primary aim in safeguarding, but a damaged reputation can mean that we won't be trusted to do the good things that we want to do within our communities.

So, let's finish this module by returning to our audit on page eight, the section on conduct. As always, look through the section and ask any clarifying questions you have.

In summary, tell your safeguarding lead about any concerning online conduct. Pass on concerns, however small, don't wait to be sure.

Do you have codes of conduct that include online behaviours as appropriate? Do you have suitable training and induction, so people understand the codes of conduct? We need to communicate the expectations for all and to all - not just for staff and volunteers, but also ground rules and group agreements for all activities, telling people what they can expect from us and vice versa.

We can model safe behaviours in our own online conduct and, where appropriate, being explicit and explaining why we're doing things in the way we are. We can equip children and young people to speak out. And we can respond in ways that reduce shame.

Our safeguarding policies and procedures should include how to report unsafe behaviour: always tell your safeguarding lead. The safeguarding lead will report to statutory agencies if a crime has been committed, or a child or at-risk adult is

at risk of harm, or a person in a position of trust is engaging in harmful conduct. Online harm against children should be reported to CEOP. If somebody in a position of trust (within your organisation or outside it) engages in conduct that means they are unsafe to work with vulnerable groups, your safeguarding lead may have to tell the barring service of DBS in England and Wales and Northern Ireland, or PVG in Scotland. Under charity law, if harmful conduct represents a serious incident or a notifiable event, your safeguarding trustee will need to report that matter to the charity regulator.

[Module 4 – Commerce]

We're going to move on to our final ‘C’ now, which is ‘commerce’, or occasionally it's referred to as ‘contract’. This refers to any online harm that involves money. Financial abuse is a category of harm for adults in safeguarding law across the UK and financial harm is often accompanied by other forms of harm too, such as emotional abuse or neglect.

In this module, we'll consider some online financial harms to be aware of. We will explore how we can reduce risks for the vulnerable groups we work with and for our organisation itself, and recognise our organisation's safeguarding responsibilities in this area.

To start us off, we're going to look at a case study. We're going to consider Donal. We're going to read Donal's scenario, and then we will answer our questions: what are our concerns and what are our safeguarding responsibilities?

Donal is 83 and attends your seniors' lunch every Wednesday. Today he arrives late and looks flustered. When you ask if he's ok, he says: "I will be once I get this bank business sorted. They sent an email in the middle of the night - someone has used my card! I just need to type in my details so they can fix it. Trouble is, I can't remember them. I wrote the password and things in my diary but that's not in the usual drawer. I've turned the place upside down! My daughter will be over later so she can help me look. I've just come out to clear my head."

So, what are your concerns? Our primary concern is Donal's safety and wellbeing. He seems upset and any change in behaviour is something we notice in safeguarding.

This sounds like a 'phishing' scam - where perpetrators contact people, often via email, to trick them into revealing private information, such as bank details. Emails often use logos, fonts, colours etc, that can look like they come from a reputable organisation. For example, an email heading may look official at first glance, but when we hover over it, we might notice that actually the full email

address is not related to the organisation they're purporting to be from. So, they might look like they come from reputable organisations, but are actually sent from the perpetrator's account.

Another concern is the content of the email - banks don't ask for account details via email. We want to stop Donal revealing his bank details.

We might also recognise there's a risk involved in keeping passwords in a diary that can be borrowed, taken away and used by someone else. Is there potential for Donal to be at risk from other scams, as well as this one?

So, are our safeguarding responsibilities?

First of all, we respond well to Donal. We would have a calm conversation with Donal to reassure him. We might encourage him to visit his bank in person if possible, or to call them, ensuring that he called them from a number he has found on his documents, not a number given in the email.

We would also report our concern - tell our safeguarding lead.

Donal is an adult and we want to make sure safeguarding is personal for him, that he is at the centre of any processes. So, we can ask Donal what he wants to happen. Does he want to talk to his daughter about this, for example? We would

only pass on what he's told us to her with his permission and / or with advice from our safeguarding lead.

We could advise Donal to forward any suspicious emails to report@phishing.gov.uk . The National Cyber Security Center will then investigate them. If you receive suspicious text messages, you can forward, forward them for free to 7726, this will report the message to your mobile phone provider.

Later, moving on from this incident, we might build in some awareness raising sessions with our senior lunch group around online scams to help raise that awareness and empower them to safeguard themselves.

[If you've been a victim of an online scam or fraud in England, Northern Ireland or Wales, you can contact Action Fraud online, in Scotland you would contact Police Scotland.]

As we said earlier, financial harm, abuse and exploitation is named in adult safeguarding legislation across the UK (in Wales, this legislation covers children too). Abuse with a financial element can also include other forms of harm and abuse that affect adults and children. So, let's pause and consider what other online financial risks we might be aware of.

Please feel free to put them in the chat or to raise your hand and unmute.

Your answers may include phishing, as we saw in Donal's example. There could also be hoax, fraud or scam, emails and messages. This can link to romance fraud, where someone believes that they are in a relationship with someone, when actually it's very one sided, and that person is manipulating them, often for financial gain. Then sextortion, where perpetrators entice someone to make indecent images of themselves and send them to the perpetrator, and they then get used for blackmail and exploitation.

We have online exploitation, where perpetrators get children, young people, or at-risk adults to do things they wouldn't normally do through grooming and deception. For example, an online 'friend' asking a teenager to receive money into their PayPal account and then moving it to another account. This seems harmless to the young person, but actually involves them in money laundering,

something they would be less likely to agree to in the physical world. There might be other forms of blackmail and bribery you can think of too.

Online gambling is a safeguarding concern in this area when it affects vulnerable groups.

There is risk of financial abuse through online purchases. Are vulnerable groups purchasing and paying through reputable organisations and sites, or are they being enticed to send money separately and not through safe lines of

communication? An additional risk of online purchases is if someone goes to collect them, where are they going? Are they going to a safe place to collect these items.,

There are also cyber-attacks, where viruses and malware are sent into computer systems and networks to cause chaos. These may again be used as a form of bribery and blackmail and could be a safeguarding concern if it involves personal data from vulnerable groups, for example.

So, how can we reduce financial safeguarding risks? We can do this by raising awareness. We can share training, tips and safety advice within our community, including with vulnerable groups in appropriate ways, so they can safeguard themselves against some of those risks. For example, advising people to contact a person directly to confirm that they sent an email asking for payment. Or being careful when opening emails from addresses you don't recognise, or clicking on links in emails you weren't expecting, even if they seem to be from someone you know.

There are different sources of information and advice we can use to raise awareness. For example, many banks will have information they can provide to you about keeping safe online and their agreed processes. Community police will often be willing to come and talk to groups and have advice on their websites and

social media platforms. You might discuss the topic within your group activities and share any helpful links and resources, such as those in the signposting section of your handbook and the appendix on basic cyber security.

Secondly, we need to use secure settings on the devices and accounts we use to communicate within our organisations. Remember, this is a non-technical webinar, and you don't need to be an expert on cybersecurity! However, we do have a safeguarding responsibility to ensure people aren't harmed through interaction with our organisation. Have you got someone in your organisation with expertise in this area who can advise about keeping devices and systems safe? There are also several websites that offer advice and guidance.

Here are some considerations: Are we managing privacy settings on our devices and apps to have that high level of security and prevent easy searching and people being able to access and share financial details?

Have we got spam filters on emails to filter out those junk emails that might be fraudulent? We need to use strong passwords on our organisation's devices and WiFi networks. And ensure staff and volunteers know not to keep them in a diary, or use the same password for multiple systems, or passwords that are easily guessed.

Quite often, you're able to have multi-factor authentication, where two or more ways might be used to gain access to an online resource. Often, financial sites will now include this, where you might have a password and a numerical code or some letters from a part of a phrase. It might be that something sent to your phone for you to click on and enter that code. Having these different steps makes the sign-in process more secure.

When looking at websites, look for that little padlock up in the URL display at the top of your website that indicates that it's a reputable, safe website. If you do come across suspicious emails, don't open them or don't forward them. There is somewhere you can forward them to report them and the details of that are in your handbook, and our co-host may pop them into the chat.

Thirdly, you need to consider your safe storage of data. This is a safeguarding responsibility. We need to ensure that all the data usage and storage complies with the General Data Protection Regulations by following our organisation's own GDPR policy.

Cloud services can often enable secure data storage. Cloud systems mean data can be easily accessed by those who need to but it's less easy to physically lose through the theft of papers, equipment and physical hard drives.

Back-up data regularly and set systems to automatically back-up where possible. You might ensure nobody else can see your screen and lock the device when leaving it.

Use antivirus software and malware protection and ensure your devices are kept securely so they can't easily be stolen.

When sharing your screen in a virtual meeting, just ensure that only the appropriate information is visible, and people can’t see private information that shouldn't be being shared.

Additional information can be found on the Information Commissioner's Office website and there is an appendix on basic cybersecurity in your handbook.

So, what are our safeguarding responsibilities in terms of commerce? Well, let's look again at our audit on pages eight and nine, ask any questions that you might have, this is your opportunity just to clarify what we mean.

This time again, we're going to tell our safeguarding lead if we're concerned that anyone may have been targeted by a financial scam, fraud or financial harm online. Pass on concerns, however small, don’t wait to be sure.

We need to have clear policies and procedures that everyone can follow. We need safe, secure storage of data that's easily accessible by those who need it

but that will not accidentally get lost. We need regular updates and safe storage of passwords, and consider using multifactor authentication for extra security. Do you have training, support and accountability for budget holders? And more widely in our organisations we can share training and best practice, regularly working together to share stories about what you've learned.

[Conclusion]

So, let's reflect as we draw near to the end of our training. How will you make your organisation safer online? What will you do in light of this training?

You might want to review your online safety policy or create one using the audit tool.

Perhaps you will think through your activities, identify where there might be safeguarding risks, and explore how you can reduce those risks.

Who do you need to work with to make your organisation’s online life safer?

Could you encourage key people, for example a specific trustee, your safeguarding lead, your IT lead (if you have one) to sign up to online safety alerts to keep up with developments.

And please don't panic! Safeguarding is a journey. This is one step at a time. The online world is moving quickly, but openness, accountability and strong policies will stand you in good stead.

So, thank you for giving us your time today. Thank you for engaging and working with us. You might want to pause and consider one final time, what have you learned? Have you got any next steps that you want to pursue? Just take a moment to write that down if you want to.

Your feedback is important to us. So we ask that you would just fill in a brief feedback form. The link will go into the chat now, or it will come as part of an email that will also give you a link to download your certificate from this training. Thank you for joining us on this Thirtyone:eight Online Safety training. Please keep your handbook as an ongoing resource. The signposting section includes many links that can take you to specific guidance that is regularly updated and our members have access to our Knowledge Hub with a wide range of safeguarding resources to use in your community. We wish you well in your online safety journey. Thank you.