Working safely online with children and young people

See all updates

This online safety guide has been produced by Childnet International for The National Lottery Heritage Fund.

Attachment	Size
Working with children and young people online	276.59 KB
Working with children and young people online – Welsh language	260.5 KB

About this guide

Heritage can provide children and young people with exciting and innovative ways to unleash their imaginations and creativity. The internet is a fantastic tool for teaching and harnessing this creativity, communicating with others and sharing successes with the wider community.

As your organisation reaches out to your existing or new communities online, it is key that you have considered children's and young people's online safety – whether your organisation is youth-facing or not. All online activities carry a level of risk, and this guide will help you understand and manage this.

The guide is produced by Childnet International for The National Lottery Heritage Fund's Digital Skills for Heritage initiative. It is viewable below and can be downloaded as a PDF from this page.

Guide

Expand All accordions

Introduction

> *"We are developing online sessions, creating video content and creating online digital exhibitions to try and engage as many people as possible, including young people and children."*
>
> *Friends of Dundonald Castle SCIO*

Engaging your audiences online can make heritage more inclusive and accessible to a wider range of people, including children and young people. In this guide, we use 'children and young people' to refer to those under 18.

> *"We are a very small organisation and we've been able to embrace the use of technology and offer equally engaging programmes online as we do when we deliver in-person. As one of our work's main targets is to future proof children and give them the necessary skills to navigate an ever-changing world, this online engagement has opened up opportunities for some really exciting future programmes."*
>
> *A Little Learning*

We have heard from over 80 heritage organisations across the UK, who have demonstrated excellent and creative ways of engaging their audiences and given us effective examples of best practice when it comes to safeguarding children and young people online. Drawing from our own expertise as well as from the heritage sector, this guide will support you with:

- Understanding why online safety considerations are vital before you embark on your digital journey, whether or not you plan to engage with children and young people directly.
- Engaging in online activity that is as enjoyable and safe as possible for the communities you work with, and particularly children and young people.
- Checklists and useful resources.

> *"We are currently engaging our members (who are aged between 8-17) through digital conferencing so we can continue to provide our sessions and a structure for our members' lives. We would normally host our monthly sessions at a cafe in Leeds, so being able to connect with our members, who live across West Yorkshire, has been a huge boon for keeping the club active. We are experimenting with a range of ways to deliver interactive sessions, whilst prioritising safeguarding in a digital environment."*
>
> *Leeds Young Archaeologists Club*

Expand All accordions

The risks

Children and young people are often at the forefront of new technologies, trying and testing platforms, tools and services before many adults. They are often leading in creating content and can be canny and imaginative producers, consumers and communicators.

However, not all children and young people have equal access, knowledge or opportunity to technology and this can often mirror and intersect with other social disadvantage. The way in which children and young people access and navigate the internet overlaps with their offline lives in significant ways – for example, whether they have access to education or support. Additionally, parents and carers have varying levels of digital confidence, knowledge and time.

It's important that we are all aware of the issues that can arise, as any child can be at risk online. We can group these risks into four key categories which can occur on any online service or

platform such as social media, online games, websites, forums, livestreaming, video conferencing or blogs.

Four risk categories

Conduct

This includes:

- Giving away personal information online such as full name, address and other identifiable information.
- Posting or sharing things online that may for instance be offensive to others, or that they may regret afterwards.
- Feeling pressure or desire to ‘fit in’, causing young people to participate in harmful ‘challenges’ or send inappropriate content or images/videos of themselves.

It’s important for organisations to role model good behaviour and provide children and young people with positive opportunities to interact online with others.

While we should not put the responsibility on children and young people to ‘stay safe’ online, they should be equipped with skills to navigate the online world safely.

Content

This includes:

- Illegal, age-inappropriate or harmful content such as pornography or violent material, self-harm and suicide content and discriminatory content eg racist, homophobic or transphobic.
- Unreliable content such as inaccurate or misleading information.

Community, youth and heritage organisations can play an important role in supporting children and young people to access safe and reliable information, and provide support and help if they access illegal or harmful content.

Contact

Children and young people can be bullied online by their peers or adults, or contacted by those who seek to abuse, exploit or harm them. This can include:

- hate speech, abusive comments and language
- being sent, or asked to do, sexually explicit activity
- being asked for financial information

Factors such as grooming, cyberbullying and wider online friendships all come under this category. Find out more on Childnet's website.

When providing opportunities for many new people to engage and meet, it's important to provide a safe space online that has clear ground rules. It is also likely that young people will interact with people online that they don't know offline, which needs to be managed safely.

Commercialism

Online advertising and marketing can make children and young people want certain things and they can find it difficult to recognise adverts online. This can result in inadvertent purchases and pressure.

When using online platforms such as social media sites or video-hosting platforms such as YouTube, adverts and pop-ups appear. This is relevant to deciding what platform to post your content, particularly if you are using social media advertising or using tracking and cookies on your websites.

Checklist

- How much do your staff know and understand about the risks that children and young people face online?
- Does your organisation recognise online safety as a safeguarding issue?

Useful links

- Childnet have Childnet have information and advice for professionals on a variety of topics including cyberbullying, social media, sexting, gaming and livestreaming.
- Stonewall and Childnet have created a guide on supporting LGBT children online.
- NSPCC have information on keeping children safe online.
- UK Safer Internet Centre have online safety resources, helplines for support and advice on how to get involved in positive national online safety awareness campaigns.

Expand All accordions

Key steps for engaging communities online

Policies

It's important for all organisations working online to have an online safety policy in place. This will help everybody to understand their role and how they can play their part in protecting children and themselves online.

Any online safety policy should sit alongside your other safeguarding policies, as well as risk assessments, to make sure that you adopt a cohesive approach. Make use of existing templates (see useful links below) and adapt and make them relevant to your organisation and the work that you do.

It is good to consult staff, volunteers and your community, particularly young people. They may highlight areas that you may not have considered, for example, additional needs they may have.

When developing policy, consider the following:

- What current policies do you have and are they sufficient to cover your online activity?
- What is acceptable language, behaviour and conduct on your online platforms by all staff, volunteers and those who you engage with?
- Do you have policies or guidelines for the platforms you are using, such as social media, video-conferencing or live events? Are these guidelines easily accessible and easy to understand?
- How do you manage consent and share information, images and videos of your community, especially children and young people?
- Who is responsible for the policy and will lead on any safeguarding or child protection decisions?
- Do your staff know how to respond if, when communicating with children through any form of online communication (ie social media, video calls, livestreaming or calls), they suspect or are told that a child could be harmed in some way?

Tips on putting policy into practice:

1. As part of induction or updates, ensure all staff and volunteers who are working online have read your online safety and safeguarding policy or guidelines.
2. Make sure everyone understands your community engagement rules for online activity, including staff, volunteers and those you work with.
3. Let staff, volunteers and your communities know where they can go for support.
4. Your policy documents should be working and living documents. Review and update when you are making significant changes to the way you work or if an issue develops. Listen to and engage your staff, volunteers and community to help you do this.
5. What is right for another project or organisation may not be right for you and there is no easy template. You know the people that you work with best, so trust your expertise and knowledge.

> *"Having a statement for the audience to read together as an oath using age appropriate language works very well. This shows that we are all invested in safeguarding the participants. The participating children also understand what is expected of them in regards their role within the session such as 'I won't share any details with people I have never met in real life."*
>
> *Royal Museums Greenwich*

Useful links

- See the Online Compass from charity Safety and Security Online – a self-review tool to establish your online safety provision. You can also use their online safety policy templates.
- NSPCC Learning has a checklist as well as helpful Safeguarding Standards. It can be used by any organisation that works with children and young people. They also have an online

safety policy template you can adapt for your organisation.
- See Company Three's Working online risk assessment template as an example you can adapt and tailor to your own organisation.
- See the ICO's site for how to process and manage children's personal information.
- See the NSPCC's advice on what to do if a child reveals abuse.

Expand All accordions

Key advice for staff and volunteers

Operating online is about transferring the safeguarding best practice you have offline into the virtual world, making activities safe and inclusive for everyone. This is not an exhaustive list, but here are some key considerations when engaging communities online across all platforms.

Interacting with children and young people online

Involve young people

Explain and discuss your procedures with the young people you are working with and why it's important to follow them. Give them opportunities to feed in and help you develop your policies or guidelines.

Children and young people are often given rules without being given the chance to discuss them. This can be disempowering. They will also often have many good and helpful ideas.

Personal accounts

Use only work accounts, for example on social media, and ensure staff, ambassadors and volunteers don't 'friend' or add young people to their contact lists through their personal accounts. If using services such as WhatsApp to have interactions with young people, including groups, always ensure that they are via work phone numbers and devices.

This is to protect children and young people as well as to have full transparency if any complaints or issues arise. It is also to protect both staff and those who they are engaging with, as you do not want to give away personal information.

Devices

All communication with young people should be done on an organisation's device that is password protected. In very small organisations or those without work devices, it is advisable to use platforms where someone else from your team can sign in to observe the conversation as it takes place.

It's very easy for information to be backed up and stored in other places on our personal devices, sometimes without us realising. When accessing, managing and storing young people's data we have to be careful to protect it.

One-to-one interaction

Avoid having unnecessary one-to-one contact with children and young people through any online medium. In situations where this might or does happen, make sure you have the consent of their parents or carers and they are aware of when and how long you will be engaging with them, as well as the focus of your discussion or session.

If you are emailing a child or young person, always copy in another member of your team and explain to the young person that you will do so. Often, young people may forget to ‘Reply All’ when they respond, but ensure that you keep other staff members involved.

Making sure that there is transparency and accountability for any conversations you have with young people is key.

Group discussions

If you are having online group discussions or sessions, think about who is involved, their ages, how they will interact and know each other.

It’s really important to set ground rules. Ask the young people what they think and to set them with you. Make sure that all participants know them. Not all young people will be equally as confident to speak up on a group discussion. Try to provide young people with as much information and prompt questions before the discussion as well as alternative ways they can be involved.

You might be introducing new young people to each other. How they will interact with each other is really important as they may start interacting outside of your discussions.

Working as an organisation online – accounts, devices and security

Accounts

When using a new online platform or service, make sure all your staff and volunteers are using accounts that are in your organisation’s name and set up for purely professional purposes.

Devices

Try to provide staff with devices (laptops, phones) that are for work purposes only. If this is not possible, establish clear guidelines how they will interact with others, protect organisational information, data and personal information of others.

Personal use

Organisational accounts should not be used for personal purposes, for example, using a Zoom account for personal use.

Why it's important

To protect your organisation’s reputation, the personal information of your staff and volunteers, and to ensure transparency and accountability. Furthermore, you want to be able to own any content or information that is created or shared online. To do so, the organisation needs access.

Working as an organisation online – security

Passwords

Make sure that all your accounts have strong, secure passwords using a mixture of lower and upper case letters, symbols and numbers. Change passwords regularly. Don’t share your passwords or logins with others. Make sure passwords are unique to the account or service you are using.

Many accounts get ‘hacked’ by people who guess the password. If someone accesses your account, they could access personal information or post offensive or illegal content from it.

Remote working

If staff or volunteers are working remotely, ensure that any work devices are closed when they are not using them and are password protected.

Closing or logging out of devices ensures they are locked and can’t be used by others, and that any in-built camera is not active.

Updates

Remind your staff and volunteers to update software regularly, as there may be new security updates.

Technology changes rapidly. It’s important to keep updating your software to ensure that you have the most secure version.

Useful links

- Digital Youth Work is an EU project supporting organisations to engage with young people online.
- Childnet's Using technology safely checklist.
- Password management and security guide – South West Grid for Learning.

Expand All accordions

What do I need to know about using social media for my organisation?

Social media is a highly effective way to showcase your work and have dynamic and ongoing conversations with your audiences and communities. You could host live Q&As on Twitter, ask your

audiences for reviews, or go live on Instagram Stories. It’s also a wonderful way to empower and include your audiences.

Do your research

Think about which platform and tool is best for your organisation and what you want to achieve. One social media service may be better suited for your communities than others. Think about how children and young people may engage with your social media activity, whether you are targeting them or not.

You can use social media to broadcast or promote your work – providing updates, showcasing your work or reaching new people.

You can also communicate with a group – an online group or page that shares information and stays connected. On many sites you can choose who is in these groups and limit it to specific people.

Once you’ve decided on the best platform, learn the safety tools and the rules. Most platforms will have a help centre.

Think about how you will moderate comments or interactions, particularly from children and young people, and if you have capacity to do so regularly. Some services such as YouTube enable you to disable comments, for example.

Establish guidelines

The content you post and share on social media, as well as your tone of voice, should reflect your activities, aims and values as an organisation.

Make sure your staff and volunteers are clear about your organisation’s expectations of how they should behave online, including what they ‘post’, ‘like’, ‘reshare’ or ‘retweet’. This is particularly crucial if you are likely to be engaging children and young people. Consider adding social media use in your staff or volunteer code of conduct or behaviour policy.

> *"We use a business page on Instagram and a page on Facebook rather than personal accounts and they are branded with our business name. We keep posts appropriate and relevant and we do not share personal information about participants."*
>
> *Just Curious Club*

Security and settings

Make sure you understand the privacy settings of any social media service you are using. Privacy settings allow you to select the audience for everything you post or share, as well as define what other apps or services can see. It is most likely that you want your organisation’s account to be public, but it’s important to be aware of all the options.

Your staff may post from their own phones/tablets to your social media accounts so they can post quickly, particularly on platforms such as Instagram or Snapchat. If this is the case, they should take care to logout of online accounts, especially if working remotely. Take steps to secure any organisational accounts and devices to prevent unauthorised or accidental access.

Social media and engaging children and young people

Social media apps such as Instagram, Snapchat and TikTok are incredibly popular with young people, including those of a primary age. These types of sites allow young people to be creative online, keep in touch with their friends, share photos and videos and much more. Many sites have a minimum user age of 13, although some interactive sites, such as LEGO Life and PopJam, are specifically designed for younger children.

Whether you are looking to use social media to engage directly with young people, or to broadcast to an audience that might include young people, you should be aware that most social media sites are only for those 13+, with platforms such as WhatsApp being 16+. Social media sites often have additional layers of protection for users aged between 13 and 18, including who can view their profiles and send friend requests etc.

It's important to recognise that while many children may use social media platforms under the age of 13, they are going against the terms and conditions of the platform.

If you are actively engaging with young people under the age of 13, it is best not to use social media platforms to do so. There are alternative child friendly platforms such as YouTube Kids. Or you can use platforms such as Basecamp (for all ages) or Slack (16+ only).

Don't forget:

- Only engage through organisational accounts, not personal ones.
- Remind the young people that what they share is on a public platform and can be seen and screenshotted by many people that they or you don't know.
- Make sure young people know where and how they can report if they receive negative comments, are targeted or see any upsetting content.

See the reporting section in this guide to find where young people can get help.

Creating content with children and young people

You will need the child's consent and the consent of the parent/carer in order to share children and young people's content online, via a consent form or email exchange, for example. Make sure you build this in at the beginning of the process. Then make sure the child is happy with the final version/edit and seek consent from their parents/carers as well.

Some key points if you are sharing content involving children and young people on social media:

- Do not use the child's surname and any other identifiable personal information.

- Children and young people’s content should only be shared through the official organisation account.
- If content created by young people is hosted on their personal social media accounts, and you don’t have their and their parents/guardian’s consent, don’t reshare/retweet.
- To showcase the work that young people have done, ask them to submit to you and, with their permission, you can share it on your organisational account.

Checklist

- Explore the platforms and services you want to use and how they will enhance the work of your organisation, as well as reporting mechanisms.
- Establish guidelines including how your organisation will use social media and communicate appropriately and safely to your audiences.
- Be mindful of age restrictions on platforms if you are trying to engage younger audiences. Most social media services are only for those 13+, with WhatsApp being 16+.
- Review and check the security and settings of the platforms you use. Do a regular check of passwords and plan how you will store and share safely.
- Set clear policies for personal use of accounts and devices and particularly for interacting with children and young people.
- Establish a clear process for obtaining consent from children and young people when sharing content on social media.
- Share content involving children and young people safely and appropriately.

> *"We send out guidance for all projects involving social media and make people aware of safeguarding resources. We monitor our social media and report accounts that are misusing our hashtags etc. We have crisis comms plans in place for difficult situations. Our Youth Panel have a social media code of practice which they jointly created."*
>
> *Kids in Museums*

Useful links

- The NCVO have a helpful guide on how to choose the right social media platform for your organisation.
- Find links to social media guides at the UK Safer Internet Centre website.
- NCVO have guidelines on how to create a social media policy.
- Find more about how young people use social media and the risks.
- See Youth Link Scotland's guide for youth workers using social media.
- Read the BBC Editorial Guidelines on children and young people as contributors.

Expand All accordions

Creating and viewing content – images and videos

Taking pictures and creating short films is easier than ever before. From taking photos and films on mobiles and tablets to creating full length films, young people are creating exciting new content on a daily basis.

Whilst the spontaneity and ease allows for innovative and creative outputs, it's also really important that everyone is clear about their rights and responsibilities regarding taking images and videos.

Get active and informed consent

Make sure that your organisation is role modelling best practice when it comes to seeking active and informed consent in sharing images and videos publicly online.

Before videoing or photographing young people, or publishing or posting, ensure you are clear about your organisation's policy and that they and their parents and carers have completed relevant consent forms. If you are asking young people to submit photos or videos of themselves that they have taken, it is still essential to obtain consent and keep a record.

Children and young people also have the right to withdraw consent at any time, and it's good to have a process in place to do this if they wish.

Take and store content safely and securely

It is advisable to only use organisational devices to capture images or videos of children.

Consider where videos and images will be stored and how long for. When saving a file, ensure this is on a secure network or encrypted USB, and then deleted when no longer required.

Think about how and where to share content

Consider appropriateness of the image or video before sharing. If a photo or video that has been submitted causes concern (or is potentially illegal) follow your organisation's safeguarding policy.

It is best practice not to share the image or video with the child's full name, or other relevant personal information, in order to safeguard their welfare.

Checklist

- Do you obtain active consent from anyone you are filming or photographing, or if they are submitting content to you?
- Is there a process for how images and videos are taken, stored and kept, particularly of children and young people?
- How and where are images and videos shared? Is there particular care not to publicly share children's personal information?

Useful link

- NSPCC have a photography and filming policy statement that you can use and adapt.

Expand All accordions

Hosting live online events

From live concerts to panel discussions, many organisations host live events, workshops, webinars and Q&As. There are many benefits to holding an online event. You can open your event to many more people than could attend otherwise. You can also use the social and chat tools to keep the conversation about the event going and make it more inclusive and open.

When hosting a live event it is important to think about the safety of your audience members as well as any staff, or invited guests or artists.

Whether you want to reach a wider audience with a livestream broadcast or small audience through a webinar, or you want to prioritise audience participation, there are a wide range of platforms for different events. Which platform you choose will depend on what you want from the event, how regularly you want to host it and who your audience is.

When deciding on your platform and format, some points to consider include:

- What is the intended age of your audience? Are they allowed to be on the platform you have chosen? If your audience members are under 13, it is not advisable to use Instagram Live, for example.
- Think about whether any of your audiences will be excluded by the platform or tools used. Have you asked them if they have access?
- Provide clear and simple instructions on how to join and participate.

> *"Be confident about using new platforms, practice in advance and do 'housekeeping' – how to talk in a group/remind people how to mute and unmute, etc. Helping people to understand how to communicate online will make the meeting/online engagement less awkward and more rewarding for all."*
>
> *Amgueddfa Cymru – National Museum Wales*

Check the platform of choice

Conduct a comprehensive audit and list any potential benefits as well as risks. Areas to consider are:

- Who can get access, join the event and how?
- What is the age limit of the platform? Do users have to create an account?
- Is the event public or limited to those who register?
- Once the event is happening, who can see what?
- Can participants join the conversation? Is this via microphone or live chat? If via microphone, what muting options will be required?

- If you are enabling a live chat, can participants privately message each other? Can all participants see the conversation, or do you want to limit it?
- Who can share content or start a stream?

What your ground rules should include

Just like you may do in an offline event, make sure there are clear safety and ground rules for your event. In an offline event, you may communicate the fire exits and toilets – think about what the virtual version is.

- Do your staff have a safe and appropriate place to share live video streams from without inappropriate objects/personal information visible?
- If you are sharing your screen, are you confident that there is nothing on your screen that is inappropriate or giving information you don't want to share (for example, personal information)?
- If you are working with children or young people, think about how they will be supervised during the calls. Do you want parents and carers to remain in the room? Do you request that they take the call from a shared space, such as a living room rather than a bedroom?
- Clearly communicate what kind of language and behaviour is expected and acceptable. For example, you could gently remind parents and carers to make sure all their children and young people are appropriately dressed if they are coming on screen. You might also want to start the session reminding everyone who is on the session and to be mindful of their language, especially if small children are present.
- Be firm and clear about any sanctions if your viewers breach any of your guidelines and explain it is to protect your community.
- Your platform might allow participants to directly message a host if they have a concern. If you are hosting to a large group, you might want to draw their attention to the reporting functions of the site.
- Think about how you will manage the risk of recording and screen shots being taken. If you are recording the event then let all your viewers know.
- If the event is public where you don't know your audience members, remind your viewers that this is the case and to come to you or report to the service provider if they have any concerns about another viewer. This is particularly important if children and adults are interacting online through your event.

> *"We have faced accessibility issues with engaging participants in remote activities, such as access to a laptop or suitable Wi-Fi connection at the time of live session. To combat this, we record all sessions and send them to registered participants so that they can join in the activity at any stage during that week."*
>
> *Nerve Centre*

Ensure you have capacity to manage the event

If possible, always have at least two people managing an event – one to present and one to manage the chat room and troubleshoot. If you are using 'closed' rooms or calls on platforms such

as Zoom or Skype and working with children and young people, try not to be left alone with a young person on the chat room or call.

Discuss and make sure you agree beforehand what you would do if the event was disrupted or hacked and who is responsible for taking that action and carrying it out. They might have to act very quickly. If anything happens where illegal or very harmful content is shared, the best course of action is usually to shut the event down.

Your audiences will appreciate that you take such behaviour seriously, rather than attempt to continue. You can always follow up with your audiences and explain your actions were to keep them safe.

Live Q+As and chat are an inclusive way to engage your audiences and ensure that the event is stimulating and interesting. Make sure that you have a dedicated member of staff managing and moderating this, with administrator or moderator privileges, so they can help the questions keep on topic and flowing.

If there are users being purposefully disruptive on a public site such as Facebook Live, it may be better not to interact with them, but post messages and content so that the comments are out of view. You can also report the user to the platform or site.

> *"We remove all private chat except for private chat to the host of the session. We have three staff monitoring the session. One to lead the session and one to monitor the language in the public chat room. The third member works as a liaison between the audience and the facilitator, keeping an eye out for any concerns or opportunities to engage the participants into the session through the public chat room."*
>
> *Royal Museums Greenwich*

Admins, moderators and contributors

There is a lot of terminology when managing or hosting events and these vary across services. If you are running an event, whether it’s on Instagram Live, Zoom or Google Hangouts, check the different roles and the powers you have. For example, can you:

- Block, remove or report users?
- Add or manage new people joining?
- Share screens and manage who else can do so?
- Mute participants, or even disable spoken chat?

Trial it with some colleagues or volunteers and play around with the settings before you do it for real.

Checklist

- How have you decided on your chosen platform and are you aware of the various settings and controls?
- Is there enough capacity to manage and moderate your live event safely?
- Are there ground rules for your live event and clear instructions on where your viewers can go if they have concerns or complaints?

Useful links

- Unesco have some helpful links to distance learning platforms.
- UK Safer Internet Centre advice on safe remote learning.
- Childnet have helpful advice for professionals working with young people on livestreaming and video chat and webcams. You might want to give the young people you work with some tips and help.

Expand All accordions

Reporting and responding

It's vital that everyone in your organisation knows what to do, and is comfortable to report, if online safeguarding concerns do arise.

Where young people can get support

It's crucial that children and young people are regularly reminded where they can get support and help. Even if what they are experiencing is not a safeguarding concern, they may still need support.

If a young person is upset about anything concerning themselves or a friend, there are some key places to go. Encourage them to speak to an adult that they trust about it.

Organisations to signpost children and young people include:

- Childline – free, anonymous support for under 19s. You can call 0800 1111 or chat online.
- The Mix – free, anonymous support for under 25s. You can call 0808 808 4994 or chat online.
- Childnet – young people aged 11-18 can find links to other helplines.
- Young Minds – provide support with mental health and wellbeing.
- Report Harmful Content – anyone aged 13+ can access Report Harmful Content to report concerns if they are unhappy with the way an online site or service has handled their report.

> *"The adults leading sessions may find themselves as one of the few trusted adults facilitating regular interactions with young people experiencing heightened anxiety or stress, or coming to terms with illness or even loss of people they know. We can't expect our team to become counsellors overnight, but want to upskill their understanding of young people's mental health, how to support it in practical ways, and where to signpost towards if any serious issues arise."*

Preparing you to respond effectively

If a child discloses something to a member of your staff, or if they spot an issue themselves related to the internet or use of technology, then the same reporting procedures used for any safeguarding incident offline can and should be followed. Being prepared and having appropriate policies in place will help you respond effectively.

Key questions to address include:

- Is there a clear and easy to use reporting process in place for staff that is widely known and used where appropriate?
- Are your audiences, particularly children and young people, aware of what they can do if something you are hosting or delivering online upsets or worries them in any way?
- Are reports recorded, acted upon and monitored?
- Do all your staff, volunteers and audiences know what would happen if their online behaviour went against your guidelines, and do they know where to find these guidelines?
- Does your organisation actively signpost further support to children and young people if appropriate?

Escalating a safeguarding concern

Following your safeguarding procedures, you may need to escalate your concerns to these organisations:

Grooming or other illegal behaviour

If someone is behaving suspiciously online towards a child, you should in an emergency contact the emergency services by calling 999, or otherwise make a report to the National Crime Agency's CEOP Command.

Child sexual abuse content online

This should be reported to the Internet Watch Foundation (IWF). Do not save or share this content with others as it is a criminal offence to possess or share child sexual abuse content.

Online content which incites hatred

Report this to True Vision, which tackles all forms of hate crime, including those on the grounds of race, religion, sexual orientation, disability and transgender identity.

Harmful content which is not illegal

To report this, you can get advice and support from Report Harmful Content. You can also submit a report to them if you have already made a report to an online service and are not happy with the

outcome.

Terrorism

Report terrorism related content to the police's Counter Terrorism Internet Referral Unit.

Professionals Online Safety Helpline (POSH)

If you are an organisation and have an online safeguarding concern regarding a child, you can contact the Professionals Online Safety Helpline. They can support and advise you on the best course of action:

- email: helpline@saferinternet.org.uk
- telephone: 0344 3814 772

Expand All accordions

Sharing this guide

Expand All accordions

Digital Skills for Heritage

The coronavirus (COVID-19) pandemic has made the need for organisations to understand and make use of digital more pressing than ever.

We are working with our partners to better meet the new and emerging needs of the heritage sector. We also want to help organisations develop the skills that will build their resilience long term.