Action for Children's Arts

Online Safety Policy

Schedule for Development/Monitoring/Review:

This online safety policy was approved by the Board of Trustees on:	Insert date
The implementation of this online safety policy will be monitored by: Online Safety Sub-Committee	● Janna Balham (Designated Safeguarding Lead) ● Vicky Ireland (Designated Safeguarding Deputy) ● Mimi Doulton (Online Safety Lead) ● Simon Bates (ACA Trustee)
Monitoring will take place at regular intervals:	Once a year
The Board of Trustees will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Nov 2021 and then annually
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Nov 2021
Should serious online safety incidents take place, the following external persons/agencies should be informed:	ACA Safeguarding and Child Protection Lead LADO, Police

ACA will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of
  - Participants/members
  - parents/carers
  - staff

Contents

1. Aims

This policy aims to:

- Set out expectations for Action for Children's Arts, its staff and member's online behaviour, attitudes and activities when using digital technology.
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of our charity and regardless of device or platform.
- Facilitate the safe, responsible and respectful use of technology to support ACA's activities and campaigns.
- Help staff and those working with children/young people to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of ACA upholding and protecting our reputation
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to our other policies such as Safeguarding and Child Protection or Data Protection Policy)

2. Introduction

As stated in the DfE's Keeping Children Safe in Education - Statutory guidance for Schools and Colleges:

'The use of technology has become a significant component of many safeguarding issues… The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

These three areas remain a helpful way to understand the risks and potential response. They do not stand in isolation and it is important to understand the interplay between all three.

3. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within ACA.

Board of Trustees

The Board of Trustees are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by a sub-committee receiving regular information about online safety incidents and monitoring reports.

The Board will agree to

- regular meetings with the Sub-Committee
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Trustees/External Agencies/LA's

The Charity Leader

- The Leader (Chairperson of ACA) has overall responsibility for ensuring the safety and online safety of staff, volunteers and members online, though the day to day responsibility for online safety may be delegated to others (Designated Safeguarding Lead/Online Safety Lead/Trustees)
- The Leader (and deputy Vice Chairperson of ACA) should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of

staff, volunteer/member. (See flow chart on dealing with online safety incidents – included in a later section).

Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

The person should have the following responsibilities and work with the designated Online Safety Lead to:

- keep up-to-date with developments in online safety
- ensure that staff have an up-to-date awareness of the group's current online safety policy and practices and ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- ensure provision of training and advice for staff and volunteers

Online Safety Lead

It is recommended that there should be a named member of staff with a day-to-day responsibility for online safety.

Where relevant this person should have the following responsibilities:

- takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the online safety policies and procedures along with the Designated Safeguarding Lead.
- offers advice and support for all users
- keeps up-to-date with developments in online safety
- knows where to obtain additional support and where to report issues
- reports incidents of abuse or misuse to Designated Safeguarding Lead to escalate as appropriate
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- where appropriate, communicates with parents and carers and helps parents to understand online issues through resources, websites and information about online safety.
- liaises with technical staff

Technical staff

Those with technical responsibilities are responsible for ensuring:

- that ACA's infrastructure is secure and is not open to misuse or malicious attack
- that ACA meets required online safety technical requirements and any Local Authority online safety guidance.
- that they report any suspected misuse or problems to the Leader, Designated Safeguarding Lead or Online Safety Lead

Young People

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know who to speak to if they are concerned
- should know and be made aware of responsibilities on the taking/using/sharing of images and on online-bullying.
- should understand the importance of adopting good online safety practice and positive online behaviour
- should agree to follow the group code of conduct and behaviour agreement (Acceptable Use Agreement)

Parents and Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. ACA will take every opportunity to help parents understand these issues through resources, websites and information about online safety.

- Parents/Carers need to sign and give consent for their child/young person to attend online sessions
- Parents should be present during the session either attending the session with their child or in the same room with their child while the session is taking place.
- Parents are responsible for ensuring the safety of devices in the home used by the child/young person for online activities with ACA.

4. Code of Conduct for ACA staff working with Children/Young People Online

This code of conduct must be adhered to by all adults/staff/volunteers working with children and young people and is in line with our Safeguarding and Child Protection Policy. It is important to understand that safeguarding issues remain the same, it is simply that technology provides additional means for safeguarding issues to develop. Adults using digital technology to engage with children and young people should be made aware of the potential risks that may arise.

This code of conduct aims to protect children and young people from online abuse and harm and reduce the risk of unfounded allegations being made.

The role of staff and volunteers

When working with or for children and young people, you are acting in a position of trust. You are likely to be seen as a role model and must act appropriately.

Responsibility

You are responsible for:

- prioritising the welfare of children and young people
- providing a safe environment for children and young people. This includes:
    - ensuring equipment is used safely and for its intended purpose
    - having good awareness of issues to do with safeguarding and child protection and taking action when appropriate
- following our principles, policies and procedures
    - This includes policies and procedures for child protection/safeguarding, whistleblowing and e-safety
- staying within the law at all times
- modelling good behaviour for children and young people to follow
- challenging all unacceptable behaviour and reporting any breaches of the behaviour code to the Child Protection Officer
- reporting all allegations/suspicions of abuse following our reporting procedures. This includes abusive behaviour being displayed by an adult or child and directed at anybody of any age.

Rights

You should:

- treat children and young people fairly and without prejudice or discrimination
- understand that children and young people are individuals with individual needs
- respect differences in gender, gender identity, sexual orientation, culture, race, ethnicity, disability and religious belief systems between yourself and others, and appreciate that all participants bring something valuable and different to the group
- challenge discrimination and prejudice
- encourage young people and adults to speak out about attitudes or behaviour that makes them uncomfortable.

Relationships

You should:

- promote relationships that are based on openness, honesty, trust and respect
- avoid favouritism
- be patient with others
- use special caution when you are discussing sensitive issues with children or young people
- ensure your contact with children and young people is appropriate and relevant to the work of the project you are involved in
- ensure there is always more than one adult present during activities with children and young people
    - if this isn't possible, ensure that you are within sight or hearing of other adults
- only provide personal care in an emergency and make sure there is more than one adult present if possible.

Respect

You should:

- listen to and respect children at all times
- value and take children's contributions seriously, actively involving them in planning activities wherever possible
- respect a young person's right to personal privacy as far as possible
    - in some cases it may be necessary to break confidentiality in order to follow child protection procedures; if this is the case it is important to explain this to the child or young person at the earliest opportunity.

Unacceptable behaviour

When working with children and young people, you must not:

- allow concerns or allegations to go unreported
- take unnecessary risks
- smoke, consume alcohol or use illegal substances
- develop inappropriate relationships with children and young people
- make inappropriate promises to children and young people
- engage in behaviour that is in any way abusive
    - this includes having any form of sexual contact with a child or young person
- let children and young people have your personal contact details (mobile number, email or address) or have contact with them via a personal social media account
- act in a way that can be perceived as threatening or intrusive

- patronise or belittle children and young people
- make sarcastic, insensitive, derogatory or sexually suggestive comments or gestures to or in front of children and young people.

Upholding this code of behaviour

You should always follow this code of behaviour and never rely on your reputation or that of ACA to protect you. If you have behaved inappropriately you will be subject to our disciplinary procedures. We may also make a referral to statutory agencies such as the police and/or the local authority children's social care department.

If you become aware of any breaches of this code, you must report them to the Designated Safeguarding Leads.

5. Safety Principles

Government guidance advises organisations follow these six key safety principles when working with children and young people online

1. **Managing Content on Our Service**

- Decide what content is acceptable on our service, and how we'll make this clear to users.
- Be clear on minimum age limits and discourage those who are too young.
- Consider different default protections for accounts that are opened by under 18s.
- Plan and regularly update how we'll manage inappropriate or illegal content posted on our site.
- Consider using available age verification and identity authentication solutions.
- Plan now for dealing with illegal content.
- For under-13s, consider pre-moderating content before users see it. Also become familiar with the UK rules to advertising to children.

2. **Parental Controls**

- Consider parental controls that are designed for our service.
- Be aware how different parental controls might interact with our website.

3. **Dealing with Abuse/Misuse**

- Explain to users the type of behaviour we do and don't allow on our service.
- Make it easy for users to report problem content to us.
- Create a triage system to deal with content reports.
- Work with experts to give users additional information and local support.
- For under-13s, speak in their language, and pre- and post-moderate their content.

4. Dealing with Child Sexual Abuse Content and Illegal Contact

- Give our users a standardised function for them to report child sexual abuse content and illegal sexual contact.
- Have a specialist team, who are themselves supported, to review these reports.
- Consider technology such as PhotoDNA and working with relevant bodies such as the Internet Watch Foundation (IWF) to help remove child sexual abuse content.
- Escalate reports of child sexual abuse content and illegal sexual contact to the appropriate channel for investigation.
- Tell users how they can report child sexual abuse content or illegal sexual contact directly to the relevant authorities and/or where to obtain further advice.

5. Privacy and Controls

- Only collect the personal data we actually need for our service.
- Tell users what information we collect, why and how long we'll keep it.
- Give users reasonable choices about how to use their personal information and specific types of data, such as geolocation data.
- Offer privacy settings options, including privacy-by-default, to give control to our users.
- Involve parents/guardians if we collect personal data from under-18s.
- For under-13s, have stricter privacy measures to help them understand the implications of sharing information.

6. Education and Awareness

- Educate users about safety as part of the experience on our platform.
- Work with parents, educators, users and their communities to raise awareness about online child safety.
- Work with experts to help develop our messages and to reach different communities.
- For under-13s, tailor the language and approach so they will take an interest.

6. Online Delivery

Our online delivery is hosted via Zoom.

- A risk assessment is carried out prior to any online delivery. This is put together in consultation with relevant staff/ACA guest speakers /participants taking into consideration our Online Safety Policy and Safeguarding and Child Protection Policy procedures.
- Two members of staff will always be present to host and co-host the call and be responsible for moderating content and dealing with any issues that arise.
- The waiting room will be used as a holding space and only known participants who have registered for the call will be permitted entry.

- While in the waiting room the host will amend participants' names if they are children or young people under 18 to only include first names in line with our child protection policy.
- The host will ensure that Zoom private messaging and screen sharing is disabled so that no unnoticed communications can take place between participants.
- Parents will have given signed consent for children under 18 to attend the call and will sign the Code of Conduct (Acceptable Use Agreement) on behalf of participants under 18. Children and young people will work to put together their own group contract to be adhered to during the call.
- At times the mute function will be utilised by the host to ensure the best quality experience for participants.
- Parents will need to be present or in the same space to supervise all online activity with children and young people under 18.

7. Handling Online Safety Concerns

Staff should recognise that online safety is a part of safeguarding.General concerns must be handled in the same way as any other safeguarding concern. Procedures for dealing with online safety will also be detailed in the following policies:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour/Code of Conduct Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day as they occur.

Any concern/allegation about staff misuse is always referred to The Leader, unless the concern is about The Leader in which case the complaint is referred to the Trustees and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

We will actively seek support from other agencies as needed (i.e. The Local Authority, LGfL, UKCCIS, UK Safer Internet Centre's Professionals' Online Safety Helpline, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or participants engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would be banned from ACA technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate when working with children and young people, either because of the age of the users or the nature of those activities.

ACA believes that the activities referred to in the following section would be inappropriate and that users, as defined below, should not engage in these activities in/or outside the organisation when using ACA equipment or systems. ACA's policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	

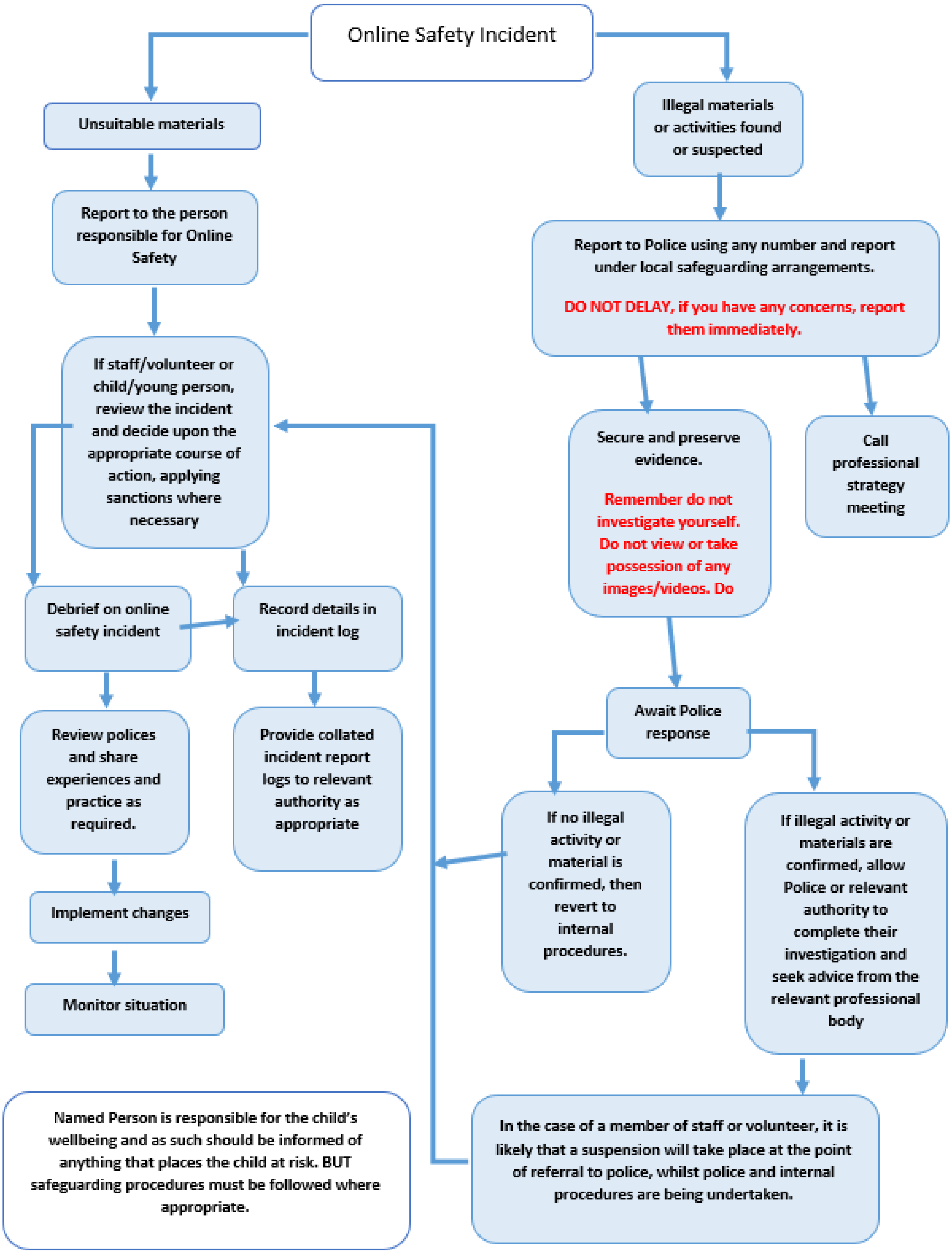
comments that contain or relate to:	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of ACA or brings ACA into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: ● Gaining unauthorised access to ACA networks, data and files, through the use of computers/devices ● Creating or propagating computer viruses or other harmful files ● Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) ● Disable/Impair/Disrupt network functionality through the use of computers/devices ● Using penetration testing equipment (without relevant permission)						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by ACA					X	
Revealing or publicising confidential or proprietary information (e.g. financial/ personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Using ACA systems to run a private business					X	
Infringing copyright					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)						
On-line gambling					X	

On-line shopping/commerce			X		
File sharing			X		
Use of social media			X		
Use of messaging apps					
Use of video broadcasting e.g. Youtube			X		

(guidance continues on next page)

8. Illegal Incidents

If there is any suspicion of illegal activity, refer to the right-hand side of the Flowchart for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

9. Sanctions

It is more likely that ACA will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that the organisation is aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Incidents	Refer to line manager/leader ma manager	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action

	manager/GrouLeader						
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	x	x	x				
Inappropriate personal use of the internet/social media/personal email	x				x	x	x
Unauthorised downloading or uploading of files	x				x	x	x
Allowing others to access ACA's network by sharing username and passwords or attempting to access or accessing the network, using another person's account	x				x	x	x
Careless use of personal data e.g. holding or transferring data in an insecure manner	x	x	x	x	x	x	x
Deliberate actions to breach data protection or network security rules	x	x	x	x	x	x	x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x	x	x	x	x	x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x			x	x	x	x
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with young people or children	x	x	x	x	x	x	x
Actions which could compromise the staff member's	x		x	x	x	x	x

professional standing							
Actions which could bring the organisation into disrepute	x	x	x	x	x	x	x
Using proxy sites or other means to subvert the filtering system	x	x	x	x	x	x	x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x	x	x	x	x
Deliberately accessing or trying to material that the group has agreed is inappropriate	x	x	x	x	x	x	x
Breaching copyright or licensing regulations	x	x	x	x	x	x	x
Continued infringements of the above, following previous warnings or sanctions	x	x		x	x	x	x

10. Parents or guardians

Parental controls help parent and guardians to block or filter upsetting or inappropriate content, and control purchases within apps. We encourage supervising adults at home to install parental control software on your child's and family's phones or tablets, games consoles, laptops and your home internet.

Parental controls can help you to:

- plan what time of day your child can go online and how long for
- create content filters to block apps that may have inappropriate content
- manage the content different family members can see.

We will signpost parent and guardians to Child Safety Online: A practical guide for parents and carers through our Online Safety Agreement for use with young people. There are also a number of resources in the Appendices.

Appendix 1 - Online safety resources for adults

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/91 2592/Keeping_children_safe_in_education_Sep_2020.pdf

https://assets.publishing.service.gov.uk/governmenploads/system/uploads/attachment_data/file/89 6323/UKCIS_Education_for_a_Connected_World_.pdf

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/81 1796/Teaching_online_safety_in_school.pdf

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/48 7973/ukccis_guide-final__3_.pdf https://learning.nspcc.org.uk/safeguarding-child-protection

https://learning.nspcc.org.uk/safeguarding-child-protection/social-media-and-online-safety

https://learning.nspcc.org.uk/safeguarding-child-protection/online-safety-for-organisations-and-groups

https://nnfestival.org.uk/festival-bridge/what-we-do/research-development/digital-resourcestoolkit/online-safety-module/

https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

https://www.saferinternet.org.uk/our-helplines

https://www.saferinternet.org.uk/hotline

https://www.internetmatters.org/resources/glossary/

https://www.childnet.com/parents-and-carers/hot-topics/

https://www.childnet.com/resources/star-sen-toolkit

https://www.artscouncil.org.uk/sites/default/files/downloadfile/Online%20Safeguarding%20Resources%20and%20Training%2012.06.2020%20Update_0.pdf

Appendix 2 - Online safety resources for young people

https://www.bbc.com/ownit/curations/bullying-and-trolling

https://www.bbc.co.uk/newsround/44074704

http://www.wisekids.org.uk/internetsafetygames.htm

https://beinternetlegends.withgoogle.com/en_uk

https://www.disrespectnobody.co.uk/

Appendix 3

Arts Council and Digital Culture Network advise using a 10 Step Plan recommended steps, with signposting to organisations, materials and templates that will help us develop our understanding in this complex area and create a culture of best practice across our organisation.

1. Review our policies. Depending upon the scale and ambitions of our online delivery, either include online safety as a section or annex within our safeguarding policy or create a separate policy for Online Safety.
2. Consider having a named individual with responsibility for online safety.
3. Depending on our delivery include some or all of the following - principles for choosing platforms or services, use of devices (personal or organisational), training (for your lead and all staff), systems for reporting and logging incidents, data storage and deletion, plus a review procedure for our provision.
4. Have an escalation plan (i.e.: know what to do and who else to involve if an incident arises). As outlined in our Child Protection and Safeguarding Policy and Procedures and MTP staff handbook.
5. Have Online Safety Agreements (i.e.: put our policy into practice to help staff/young people and parents understand their responsibilities).
6. Ensure everyone in our organisation knows how and to whom to report an issue.
7. Ensure we are GDPR compliant, particularly as we are storing young people's contact details, filming online sessions etc.
8. Refine our practice by talking to members//young people/children/parents. Discuss together and amend our delivery accordingly.
9. Keep up to date with best practice by using the widely available free resources and materials.
10. Review our policies and procedures as our digital provision grows.

Contact Details

Vicky Ireland, Chairperson ACA: vicky.ireland@childrensarts.org.uk

Janna Balham, Designated Safeguarding Lead: janna.balham@childrensarts.org.uk

Mimi Doulton, Designated Online Safety Lead: mimi.doulton@childrensarts.org.uk

Police 999 (imminent threat) or 101 (non-emergency)

NSPCC Helpline help@nspcc.org.uk 0808 800 5000