

Making the most of your of your digital content for schools

Online Safety  
*from policy to practice*



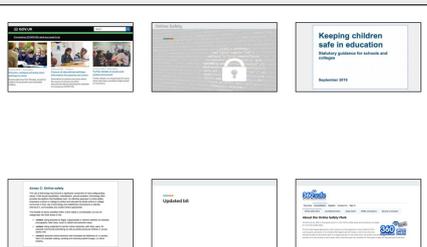
- Understand the requirements on schools
- Help you create an online safety plan
- Know where to go for help/guidance

## Toolkit



**Making the most of your digital content for schools:**  
A toolkit for arts and cultural organisations

## PDF/Slides



## Resources Page



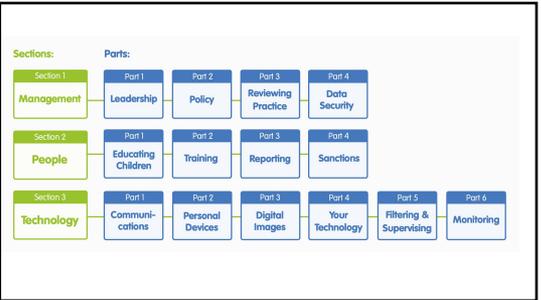
## Checklist

- Create or update policy
- Create or update Acceptable use agreements
- Agree a named lead
- Create a training and/or keeping up to date plan
- Agree a system to log incidents
- Create or update an escalation plan
- Devise a system to review and monitor
- Make sure everyone knows the plan...





<b>A. Policy &amp; Leadership</b>	<b>B. Infrastructure</b>	<b>C. Education</b>	<b>D. Standards &amp; Inspection</b>
<p><b>Leadership and Policies</b> responsibilities, policy development and scope, reporting, management of communication technologies</p> <p><b>Infrastructure</b> passwords, system security, data protection</p> <p><b>Education</b> for children, staff, parents</p> <p><b>Monitoring</b> of incidents and effectiveness of all of the above</p>			



<b>Section 1: Management</b>		Section: 1 of 3
<p>This section reflects the importance of having effective leadership; clear policies that are agreed, understood and respected by everyone and regularly reviewed. There is good practice in keeping data safe.</p> <p><b>Part 2: Policy</b> Are there policies and guidance in place for managing the online safety of all users and does everyone understand them?</p>		
<b>Red Level</b>	<p>There is no policy or guidance in place for managing the online safety of all users.</p> <p><b>How to Improve: Red to Amber</b> Develop an Acceptable Use Policy. A good starting point is to look at the SWGFL Template AUP (see links below) and to check if your local authority or other relevant local / national organisation has guidance on what an AUP should be like for a setting such as yours. It is also a good idea to check what policies and practices you already have in your organisation. The AUP should create an agreement between the organisation and users concerning expectations about safe use of ICT. Depending on your organisation you may need separate AUPs for staff use and for young people's use. You need to make sure that all legal responsibilities are covered, but the SWGFL template AUP will help with this.</p>	<p><b>What Evidence could you use?</b></p> <p>Overall vision or mission statement. E-Safety Pledge. Any existing Acceptable Use Policies. Child protection policy and procedures. Code of practice concerning behaviour. Staff / volunteer handbook and guidance on safer working practices with children. Development plan. Minutes of meetings.</p>
<b>Amber Level</b>	<p>A designated person oversees the management of the online safety of all users.</p> <p><b>How to Improve: Amber to Green</b> An AUP is a document that outlines the important rules that users need to know, understand and follow in your organisation. An online safety policy for the organisation is much wider and should cover such aspects as responsibilities, reporting, monitoring, sanctions, education, awareness raising / training. A policy is more effective if those it affects are involved in its development. It must be integrated into and consistent with other relevant policies, in particular the child protection and safeguarding policies.</p>	
<b>Green Level</b>	<p>There is a clear Online Safety Policy, supported by an agreed Acceptable Use Policy. These are integrated into the organisation's safeguarding policies. The policies are agreed and respected by all.</p>	

ROYAL OPERA HOUSE Learning Platform

OUR RESOURCES - EVENTS - Sign in Register

## The ROH Learning Platform

Bringing the world of theatre right into the classroom

ROYAL OPERA HOUSE

### E-Safety Policy

**Publishing images and videos**

- The Royal Opera House will seek permission from parents/guardians before publishing images or videos of pupils on the organization website or social media channels.
- Care will be taken that young people are appropriately dressed and are not participating in activities that might reflect badly on both the individuals and the organisation.

## Acceptable Use Agreement

**Parents/Carers:** please read and discuss this agreement with your child and then sign it, ask your child to sign it, and return it to the group leader. If you have any questions or concerns please speak to [add name/job title].

**Young person's agreement**

- I will be responsible for my behaviour when using the internet, including social media platforms, games and apps. This includes the resources I access and the language I use.
- I will not deliberately remove, download or upload material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to the group leader.
- I will not send anyone material that could be considered threatening, bullying, offensive or illegal.
- I will not give out any personal information online, such as my name, phone number or address.
- I will not reveal my passwords to anyone.
- I will not arrange a face-to-face meeting with someone I meet online unless I have discussed this with my parents and/or group leader and am accompanied by a trusted adult.
- If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I can talk to [name].

I understand that my internet use of [Name of group/organisation] will be monitored and logged and can be made available to the group leader. I understand that these rules are designed to keep me safe and that if I choose not to follow them, [Name of group/organisation] may contact my parents/carers.

**Signatures:**

We have discussed this online safety agreement and [child's name] agrees to follow the rules set out above.

Parent/Carer signature: \_\_\_\_\_ Date: \_\_\_\_\_

LGfL **DigiSafe** keeping children safe

## Acceptable Use Policy (AUP) for STAFF, GOVERNORS, VOLUNTEERS

- I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. [insert link: the LGfL DigiSafe template at safepolicies.lgfl.net includes a draft text for this.] I will report any breach of this by others or attempts by pupils to do the same to the headteacher.
- I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either. More guidance on this point can be found in this [Online Reputation](#) guidance for schools and in [insert school name] social media policy/guidance. [insert link to relevant section of full OUS policy or other policy of concern.]

## Agree a named lead/Keep up to date

UK Council for Internet Safety

Part of Department for Digital, Culture, Media & Sport - Department for Education - and Home Office

**Featured**

12 September 2019 — Policy paper

### Digital Resilience Framework

A framework and tool for organisations, policymakers, schools and companies to use to embed digital resilience thinking into products, education and services.

## Incidents and Escalation Plans



TheDigitalArtist (psabay.com)

UK Safer Internet Centre

Advice Centre Helpline Helpline Pupil powered in safety

## Professionals Online Safety Helpline

Specialist advice and online safety resources

Email [helpline@safernet.org.uk](mailto:helpline@safernet.org.uk)

Or call 0845 301 0772 (Mon-Fri 9am-5pm, Sat 10am-4pm, Monday to Friday)

Home | Professionals Online Safety Helpline

Professionals Online Safety Helpline

Are you a professional working with children and young people?

UK Safer Internet Centre

Advice Centre Hotline Helpline Pupil powered e-safety

Teachers and professionals



Home | Advice Centre | Teachers and professionals

Educators, social workers and other professionals working with children and young people play a key role in supporting children to learn about how to stay safe online.

It is our experience that this is best achieved by embedding safety across the curriculum or the work of the organisation, through a framework of effective policies and rules for reporting concerns such as cyberbullying. As well as supporting young people to stay safe online, staff also need to protect their own online reputation, particularly when using social networking sites.

*To Do List*

- Create or update policy
- Create or update Acceptable use agreements
- Agree a named lead
- Create a training and/or keeping up to date plan
- Agree a system to log incidents
- Create or update an escalation plan
- Devise a system to review and monitor
- Make sure everyone knows the plan...



Image credit: Tumisu, Pixabay

- Work through the checklist
- Don't disappear down a worm-hole
- Check out the toolkit
- Check out the resources
- Sign up to some relevant newsletters
- Share up to date information with colleagues

Digital Inequality is a thing  
Don't forget analogue

83% of 12 - 15-year-olds have their own smartphone but, as Carnegie UK Trust's 'Switched On' report highlights, connection is not the same as access

Consider providing resources which enable analogue/offline activity. PDFs and other documents have their place as settings can print them off and send them home.



Complete our survey

Thank you.

@NNFbridge  
[nnfestival.org.uk/festival-bridge](http://nnfestival.org.uk/festival-bridge)

