

Policy or Procedure Title: QSC37	<b>LAMDA Examinations Online Safety Policy</b>
Version: 1	
Owner: QSC	
Last Revised: 25.05.2020	
Review: 31.07.2020	

## **Policy Statement**

London Academy of Music and Dramatic Art (LAMDA) works with children, young people and adults at risk, delivering examinations in the UK and Internationally so that they can develop a broad range of skills that will serve them throughout life. This can only be achieved in an atmosphere of trust, respect, safety and security. LAMDA is therefore committed to creating an environment which ensures all children and adults at risk can learn and develop and one that prevents risk from any form of harm or abuse.

LAMDA has a responsibility to safeguard and promote the welfare of all children and adults at risk to whom it provides services. In recognising this duty of care, LAMDA has developed this policy with the NSPCC to provide a clear framework on our approach to online safety and ensuring children and adults at risk are safeguarded through our varied activities across LAMDA.

## **Legislation and Guidance**

LAMDA's policy is underpinned by English legislation and statutory guidance. It seeks to protect children and vulnerable adults in the UK and Internationally. Summaries of the key legislation and guidance include:

UK Council for Child Internet Safety (UKCCIS)  
Children's Online Privacy and Protection Act of 1998 (COPPA)  
UN Convention on the Rights of the Child 1991  
Data Protection Act 1998  
Children Act 1989 and 2004  
Sexual Offences Act 2003  
Working Together to Safeguard Children & HM Government (2015)  
What to do if you are Worried a Child may be being Abused HM Government (2015)  
Care Act 2014  
Mental Capacity Act 2005  
Human Rights Act 1998  
The SEND codes of Practice 2014  
Children and Families Act 2014 (for young adults 18-25)  
Protection of Freedoms Act 2012  
Counter Terrorism and Security Act 2015  
Charity Commission Guidance; The Essential Trustee 2015  
Serious Crime Act 2015

**[learning.nspcc.org.uk](http://learning.nspcc.org.uk)**

## **Definitions**

**Online** – this is defined as forums allowing digital communication, such as:

- social networks
- text messages and messaging apps
- email and private messaging
- online chats
- comments on live streaming sites

- voice chat in games

**Online risk** - this can be classified in three ways:

**Content risk:** children receiving mass-distributed content. This may expose them to age inappropriate material such as pornography, extreme violence, or content involving hate speech and radicalisation.

**Conduct risk:** children participating in an interactive situation. This includes bullying, sexting, harassing, being aggressive or stalking; or promoting harmful behaviour such as self-harm, suicide, pro-anorexia, bulimia, illegal drug use or imitating dangerous behaviour. A child's own conduct online can also make them vulnerable - for example, by over-sharing their personal information or by harassing or bullying themselves.

**Contact risk:** children being victims of interactive situations. This includes being bullied, harassed or stalked; meeting strangers; threats to privacy, identity and reputation (for example, through embarrassing photos shared without permission, a house location being identified, someone impersonating a user, users sharing information with strangers); and violence, threats and abuse directly aimed at individual users and/or groups of users.

**Illegal contact, conduct and content** - Some online risks can not only lead to harm, but also result in illegal activity. This can occur both online and offline. These can include:

- sexual grooming and sexual exploitation;
- sexting (pressure or coercion to create sexual images)
- creation and distribution of child abuse images
- Bullying / cyberbullying
- emotional abuse (this includes emotional blackmail, for example pressuring children and young people to comply with sexual requests via technology)
- physical and mental abuse of children
- online aspects of child trafficking
- selling and distributing illegal drugs

## Implementation

We believe that:

- children, young people and adults should never experience abuse of any kind
- children, young people and adults should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- the online world provides everyone with many opportunities; however, it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people and adults safe online, whether or not they are using LAMDA's network and devices
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- working in partnership with children, young people, their parents, guardians and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

We will seek to keep children and young people safe by:

- appointing an online safety coordinator
- providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and guardians to do what they can to keep their children safe online
- developing an online safety agreement for use with young people and their parents/guardians
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person
- reviewing and updating the security of our information systems regularly
- ensuring that user names, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only when appropriate
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

### **Related policies and procedures**

This policy statement should be read alongside our organisational policies and procedures, including:

- Code of Conduct
- Anti-harassment and bullying policy
- Child and Adult Safeguarding Policy
- Child Protection Policy and Procedures
- Data Protection Policy
- Digital Systems Policy
- Disciplinary Procedures
- Email and Internet Use Policy
- IT Security Policy
- Safeguarding Policy and Procedures
- Use of Social Media Policy