Online Safety Policy

This policy is written in conjunction with Keeping Children Safe in Education 2023, Cyberbullying policy, Behaviour and Code of Conduct policy, Mental health policy, PSHE RSE and the School's staff handbook.

The London Vocational Ballet School recognises that internet, mobile and digital technologies provide positive opportunities for young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all students, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

Responsibilities
The Directors and Trustees have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored.
All breaches of this policy must be reported to the Directors.
All breaches of this policy that may have put a child at risk must also be reported to Kerry Williams, the Designated Safeguarding Lead.

Legal framework
This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England.

Summaries of the key legislation and guidance are available on:
- Teaching online safety in schools - GOV.UK (www.gov.uk)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)
- Keeping children safe in education2023 - GOV.UK (www.gov.uk)

Policy and procedure
The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk. The school uses Titan security system on computers used by it's students.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for students, parents/carers, staff and governors and all other visitors to the school.

Use of email

Staff and Trustees should use a school email account for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact students, parents or conduct any school business using a personal email address. Students should use school approved accounts on the school system for educational purposes.

Staff, governors, and students should not open emails or attachments from suspect sources and should report their receipt to Kerry Williams or a member of the SMT.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Visiting online sites and downloading

Staff must preview sites, software, and apps before their use in school or before recommending them to students. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:
- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses

- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by a member of the SMT.

Storage of Images
Photographs and videos provide valuable evidence of students' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).
Photographs and images of students are only stored on the school's agreed secure networks which include some cloud based services.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with students, must only use school equipment to record images of students whether on or off site. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

Use of personal mobile devices (including phones)
The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices when necessary. Under no circumstance does the school allow a member of staff to contact a student or parent/carer using their personal email address.

Students are allowed to bring personal mobile devices/phones to school but must hand them in at the start of the day and collect them at the end of the day

Under no circumstance should students use their personal mobile devices/phones to take images of

- any other student unless they and their parents have given agreement in advance
- any member of staff

The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Curriculum

Online safety is fully embedded within our curriculum. The school provides a comprehensive age-appropriate curriculum for online safety which enables students to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE curriculum, Relationships and Health Curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

London Vocational Ballet School Online Safety Policy Statement

We believe that:

- young people should never experience abuse of any kind
- young people 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 young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep young people safe online, whether or not they are using LVBS network and devices
- all young people, 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 young people, their parents, carers 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:

- providing clear and specific directions to staff and volunteers on how to behave online through our staff handbook
- supporting and encouraging 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 carers to do what they can to keep their children safe online
- developing an online safety agreement for use with young people and their parents/carers
- 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 young people who are involved in our organisation is held securely and shared only as appropriate
- ensuring that images of 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.

Policy written by Kerry Williams – Head of Pastoral Care and Safeguarding

Approval body: LVBS Trustees

Revised date: September 2023

Review Schedule: 1 year

Next review date: September 2024