Adagio School of Performing Arts

E Safety Policy

Date: 20/10 /2021

Review Date: Autumn Term 2022

E Safety Policy

Rationale

The rapid growth of the Internet and digital electronic technology has opened an exciting world of opportunities for today's young people. It is possible for them to gain access to unlimited information worldwide, to receive entertainment via films and music and use social networking sites, allowing them to communicate easily with others. It is clear that young people use the Internet as an integral part of their learning and entertainment and this will only increase as technology and access progresses.

New technologies can offer many positive educational and social benefits to young people and the use of these exciting and innovative tools in ASOPA and at home has been shown to raise educational standards, promote creativity and effective learning.

Alongside the many benefits are a number of risks. Whilst most young people are competent in using modern technology, their understanding and management of the risks is often low. They can access digital devices in a variety of locations, some which are not in protected environments and with few controls in place.

Many adults have less understanding of the technology and are not as able in their use as young people. Therefore, they are less likely to be able to support and protect them as they might in the real world.

Raising awareness of e-safety issues and identifying and planning appropriate safeguards will help to ensure the safety of young people and give them the confidence and skills to face and deal with these risks, as well as supporting the adults around them.
Some practical examples of these dangers include:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft (including 'frape' (hacking Facebook profiles) and sharing passwords
- Being the subject of fraud

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (internet or gaming))
- Sexing (sending and receiving of personally intimate images)
- Copyright (little care or consideration for intellectual property and ownership (for example music and film)
- Plagiarism – not acknowledging sources of information copied from the internet.

Purpose

Young people need to be protected from these risks and they need to be helped to develop the skills, knowledge and awareness to keep themselves safe when they are online. ASOPA is committed to raising the awareness of E Safety issues by equipping young people with the skills and knowledge they need to use technology safely and responsibly, enabling them to manage the risks wherever and whenever they go on-line.

Scope of the Policy

E safety is concerned with **behaviour** that can be illegal, inappropriate, deliberate or accidental. It is primarily focused on protecting and safeguarding young people, but it also needs to consider how adults (staff, parents, carers, volunteers) use technology and how this impacts upon young people. E safety must be the concern of all adults, including those who do not use digital technology themselves, who may need to know how to keep children safe in the digital world.

Many of the safeguarding issues are not new – it is that they are now taking place in a different environment. This policy is about making sure that all are ready to deal with a continually changing aspect of safeguarding and child protection.

E Safety concerns **behaviours** associated with devices such as:

- Computers – desktops, laptops and tablets
- Mobile phones
- E-mail and other forms of digital communication, such as Social Networking, texting, chat and Instant Messaging
- Use of the internet (browsing, downloading, uploading and file sharing)
- Video & computer gaming, including online gaming consoles (Playstation, xbox, wii)
- Digital cameras, webcams
- IPod & mp3 music devices
- Internet enabled devices e.g. Internet tv

This policy applies to all members of the ASOPA (including staff, students, volunteers, parents/ carers, visitors) who have access to and are users of ASOPA IT systems, both in and out of College.

The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

The Strategy

Key strategy aspects

It is important that e-safety is embedded in all activities of ASOPA including safeguarding policies, practices and responsibilities.

Specific tasks include:

- To raise awareness and understanding of E safety issues amongst young people, staff, carers and parents.
- To enable staff to respond appropriately to incidents as well as to risks posed to young people by their increased use of digital technology.
- Monitor the effectiveness of the strategy itself.

E-Safety Lead

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing ASOPA's e-safety policy.
- Ensures that all staff are aware of the procedures that need to be followed in the event of a serious e-safety incident taking place (see flow chart)
- Provides training and advice for staff.
- Reports any issues through the designated lead for safeguarding

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current College e-safety policy and practices.
- They report any suspected misuse or problem to their line manager, for investigation / action / sanction.
- Staff should not disclose information such as personal email accounts or telephone numbers to students.
- e-safety issues are embedded in the curriculum and other ASOPA activities.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They are aware of e-safety issues related to the use of mobile phones, cameras, tablets and implement current ASOPA policies with regard to these devices.
- They are aware of processes in place for dealing with any unsuitable material that is found.

The Principal and designated staff for safeguarding as appropriate should be trained in e-safety issues and be aware of the potential for safeguarding issues to arise from:

- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- sexting
- sharing, loss or theft of personal data

4.2 Policy and practice

The E Safety policy outlines strategies, which support students and staff in the safe use of electronic technologies. All staff who have contact with young people should promote the safe and responsible use of technology, learn to recognise the behaviours that may indicate risky use and know where to go for help and guidance.

All staff should be aware of the appropriate response if a child or young person divulges an e safety incident, how to raise the concern and escalate it appropriately.

Policy Statements

Infrastructure

ASOPA will ensure that relevant, up-to-date and appropriate technological tools will be used to safeguard all users of the ASOPA's IT system including:

- A Firewall and virus protection.
- ASOPA retains the right to monitor email and internet access to support compliance with policies in accordance with current legislation.
- Filtering and content control to minimize access to inappropriate content.

Regulation

- All users of the ASOPA's IT system must agree to the IT User Agreement prior to being given password access to the system. Any breach of the conditions outlined in the IT User Agreement will be subject to disciplinary action through the Student Disciplinary Procedures (students) or Staff Disciplinary procedures (staff).
- An agreed policy is in place for the provision of temporary access of "guests" onto ASOPA's system, for example limited access, account expires after a specified time.
- Staff and students may formally request that IT Services Staff remove sites from the filtered list in line with the filtering policy.
- The Data Security Protocol (encompassing mobile working and remote access) informs the use of removable media (e.g. memory sticks / DVDs) on College workstations / portable devices.

Education

'E-safety is more about behaviour than technology' (Becta: Safeguarding Children on-line. March 2010).

ASOPA therefore, has a responsibility to help educate students and staff,

Students

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of the Tutorial system.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Students should be helped to understand the importance of adopting good e-safety practice when using digital technologies outside of the college.
- Conditions of use of IT Systems will be communicated to users at enrolment/induction, in the student diary, for staff on the Intranet.
- Students need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Students should know and understand college policies regarding cyber-bullying and know how to seek help, if they are affected by any form of cyberbullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent, tutor, a member of Student Support or an organisation such as Cybermentors, Childline .
- Through staff acting as good role models in their use of ICT, the internet and mobile devices.

Parents/carers

ASOPA will seek to provide information and awareness to parents and carers through the College website and appropriate events.

Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- All new staff should receive e-safety training as part of their Safeguarding Children and Vulnerable Adults training.
- To have up to date e-safety information and resources.

Management of Particular Risks

Use of digital and video images - Photographic, Video

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. For example they should recognise the risks attached to publishing their own images on the internet (social networking sites).
- Staff are allowed to take digital/video images to support educational aims, but must follow ASOPA policies concerning the sharing, distribution and publication of those images, where parental/student permission is given (on parental consent forms). Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or ASOPA into disrepute.
- Photographs published on the ASOPA's website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students must not take, use, share, publish, tag or distribute images of others without their permission.

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- ASOPA uses Facebook, Instagram and Twitter to communicate with students.
- Designated staff members have permission to set up and run social media accounts (Facebook groups) to communicate with students and in turn teach the safe and responsible use of social media sites such as Facebook.
- Students are permitted to access their personal social media account using their own device (i.e. mobile phone) outside of lessons using mobile networks (such as 3G & EE).
- Staff and students are regularly provided with information, on how to use social media responsibly and what to do if they are aware of inappropriate use by others.
- Staff and students are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever as a digital footprint.
- Staff and students are aware that their online behaviour should at all times be compatible with UK law.

Review

The e-Safety policy will be reviewed annually by the Principal.

E-Safety Policy Lead: Bronwen Patching