Online Safety, Filtering and Monitoring Policy

A. Introduction

1. The Arts Educational Schools (ArtsEd) provides a safe environment to learn, work and access its services, including when online and has comprehensive processes for its filtering and monitoring arrangements. A safe online environment, which includes effective filtering and monitoring measures, is important for the safeguarding of learners (pupils and students), staff members, hirers and visitors to protect them from potentially harmful and inappropriate online materials. To this end, ArtsEd understands the importance of having clear roles, responsibilities and strategies for delivering and maintaining effective filtering and monitoring systems within the Institution and that the professional expertise to make informed decisions about and reporting on online safety measures, including filtering and monitoring, are always available. The Institution also has comprehensive procedures for managing instances where online/ IT use expectations are not met.

2. ArtsEd's filtering and monitoring arrangements meet the regulatory requirements required by law and sector best practice. Its arrangements meet the needs of the Institution's learners (pupils and students) and staff members, as well as those who visit or access its provision, allowing the specific and appropriate use of technology while minimising potential harms.

3. Learners (pupils and students), staff members, hirers and visitors are made aware of the Institution's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to any member of the ArtsEd community. These expectations are clearly outlined in the Institution's acceptable use policies and highlighted through a variety of education and training approaches.

4. The provisions set out within this document are integrated within, and should be read alongside, the following ArtsEd Policies:
   a. IT Acceptable Use Policy
   b. Safeguarding Policy
   c. Privacy Notices
   d. Hirers
   e. Behaviour, Rewards and Sanctions Policy for Day School and Sixth Form
   f. Student Conduct and Disciplinary Procedure for Higher Education Students
   g. Anti-Harassments and Bullying Policies
   h. PSHCE Curriculum Map for Day School and Sixth Form

B. Scope

5. An active and well managed filtering and monitoring system is an important part of providing a safe environment for learners (pupils and students), staff and other users of ArtsEd's premises such as hirers and visitors. ArtsEd takes an institutional approach to online safety empowering and educating learners (pupils and students) and staff members in their use of technology and has established mechanisms to identify, intervene, and escalate any concerns of online abuse or harm, where appropriate.

6. Online abuse is any abuse that is facilitated by using internet connected technology. Online abuse may take place through social media, messaging apps, emails, online gaming, live-streaming sites or other channels of digital communication. Individuals, including children, who are abused offline may be re-victimised online if their abuse is live-streamed or recorded and uploaded online.

7. Online harm is categorised into the following areas:
    - **Content:** being exposed to illegal, inappropriate or harmful content, e.g., pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
    - **Contact**: being subjected to harmful online contact with other users, e.g., peer pressure, adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
    - **Conduct:** personal online conduct that increases the likelihood of/causes harm, e.g., making, sending and receiving consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images, online bullying, allowing apps/websites to access location, younger children sending (including inappropriate/indecent) images/information to a device's contact list (e.g., their parent's).
    - **Commerce:** commerce-based risks (both as victims and perpetrators), e.g., online gambling, inappropriate advertising, phishing and/or financial scams.

8. This policy applies to all members of ArtsEd (including staff, pupils, students, parents, visitors and trustees) and those who access our services such as hirers and any other users of the School's IT systems, both on and off site. This policy covers both fixed and mobile devices provided by ArtsEd, as well as devices owned by pupils, students or staff and brought onto ArtsEd's premises. This policy, supported by the other relevant policies listed in paragraph 4 above, seeks to protect the online safety of pupils, students and staff.

9. ArtsEd actively blocks access to sites which contain harmful content such as:- illegal child sexual abuse material, self-harm, suicide, anti-Semitic, radicalisation, extremism/terrorist content and adult content.

10. ArtsEd recognises the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace and that it is not always possible to guarantee that unsuitable material cannot be accessed via our computers or devices. To mitigate unsafe online access ArtsEd takes proactive measures to:

    a. regularly review the methods used to identify, assess and minimise online risks.
    b. examine emerging technologies for educational benefit and undertake appropriate risk assessments before use within the Institution is permitted.
    c. ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

11. The Institution is aware that no filtering and monitoring system can be entirely effective and therefore ArtsEd takes additional steps as necessary to minimise harm and meet its statutory requirements in Keeping children safe in education (KCSIE) and the Prevent duty. Where necessary, ArtsEd will refer to templates and advice in 'the reviewing online safety section' of Keeping children safe in education. Through the arrangements set out in this document ArtsEd meets the digital and technology standards set out by the Department of Education's Filtering and Monitoring Standards Guidance.

12. ArtsEd's effective filtering and monitoring arrangements aim to block internet access to harmful sites and inappropriate content in a way that does not:
    a. unreasonably impact teaching and learning or school administration.
    b. restrict learners (pupils and students) from learning how to assess and manage risk themselves.

13. All filtering and monitoring arrangements are up to date and apply to:
    a. all learners (pupils and students), staff members and guest accounts (such as visitors and hirers) ensuring all arrangements are age and ability appropriate for the users, and suitable for ArtsEd's context and an educational setting.
    b. school owned devices.
    c. devices using the school broadband connection.

14. The Institution takes steps to effectively filter all internet feeds, including any backup connections, handling multilingual web content, images, common misspellings and abbreviations as well as provide alerts when any web content has been blocked. Where mobile and/or institutionally required app technologies are used, technical monitoring systems are applied to such institutional devices to reduce the risk of harm and to ensure filtering systems are in place to identify any inappropriate content.

15. ArtsEd through its filtering and monitoring arrangements is able to identify a device name or ID, IP user address, and in certain instances, the individuals involved, the time and date of attempted access and any blocked search terms or contents.

16. All users and relevant stakeholders such as parents and carers of pupils and students under the age of 18 are informed that the use of ArtsEd's network and internet systems are monitored. The Institution also inform parents and carers of pupils and students under the age of 18 of the systems the school uses to undertake its online filtering and monitoring arrangements.

17. All filtering and monitoring arrangements are carried out by the Institution in line with the requirements and provisions of the Equality Act, Human Rights Act and General Data Protection Regulation (GDPR) and the Data Protection Act (DPA).

C. Roles and Responsibilities within ArtsEd

- **Governing Body**

i. ArtsEd's Board of Trustees

18. ArtsEd's Board of Trustees has overall strategic responsibility for ensuring online safety and are aware of the Department of Education's Filtering and Monitoring Standards Guidance. The Board receives regular assurance that the standards are being met. The Board support the Executive (Senior Leadership Board) to make sure effective online measures and filtering arrangements and monitoring strategies are in place, which meets the expected standard and the risk profile of ArtsEd. This includes procuring and ensuring the appropriate systems are in operation. The Board further supports the Executive to ensure the reporting process is effective by making sure that incidents are urgently picked up, acted on and outcomes are recorded, noting that incidents can be malicious, technical, or be of a safeguarding nature.

19. The Designated Safeguarding Trustee (DST) and the Designated Institutional Safeguarding Lead (DISL) or nominee, who is a member of the Executive, are responsible for ensuring these standards are met. The DST is responsible for regularly reporting online safety practice, incidents and outcomes including those relating to filtering and monitoring to the Board of Trustees and

relevant committees of the Board such as the Welfare, Safeguarding, Health and Safety Committee.

20. The DISL has the lead responsibility for online safety. Whilst activities of the designated safeguarding lead may be delegated by the DISL to an appropriately trained deputy, overall, the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DISL.

21. The DST and DISL or nominee will work with professional experts within ArtsEd such as the IT team and staff with Designated Safeguarding responsibilities as well as external stakeholders to ensure effective and regular filtering and monitoring are taking place and that changes are made promptly to ArtsEd's provisions, where necessary.

- **ArtsEd's Executive**

ii. Senior Leadership Board (SLB)

22. As well as working closely with the Board of Trustees, ArtsEd's Senior Leadership Board which makes up its Executive are responsible for:
    a. ensuring that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
    b. ensuring there are appropriate and up-to-date policies regarding online safety in place, including: a staff code of conduct, learner behaviour and conduct policy and Acceptable Use Policy, which covers acceptable use of technology.
    c. ensuring that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety. Please see Appendix A.
    d. supporting the DISL and the DSL/DDISL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
    e. ensuring DSSF parents and other stakeholders such as visitors and hirers are directed to online safety advice and information and provided with information on ArtsEd's website for parents and ArtsEd's community.
    f. procuring filtering and monitoring systems including, where appropriate, those which provide additional level of protection for filtering and monitoring provisions.
    g. ensuring ArtsEd arrangements meet the Broadband internet standards and Cyber security standards.
    h. documenting decisions on what is blocked or allowed and why.
    i. reviewing the effectiveness of ArtsEd's online safety provision and overseeing reports prior to these being provided to the Welfare, Safeguarding, Health and Safety Committee.
    j. ensuring all staff understand their role as it pertains to filtering and monitoring and are appropriately trained.
    k. ensuring all staff members follow policies, processes and procedures.
    l. ensuring all staff members act on reports and concerns as well as know how and where to report concerns.
    m. ensuring that appropriate risk assessments are undertaken regarding the safe use of technology.
    n. ensuring there are robust reporting channels to report online safety concerns, including internal, local and national support are available.
    o. ensuring the audit and evaluation of online safety practice to identify strengths and areas for improvement are undertaken and reported by relevant staff members.

- **ArtsEd's Staff with operational online safety responsibilities**

23. Day-to-day management of online safety, including filtering and monitoring systems, requires the specialist knowledge of both safeguarding and IT staff to be effective.

24. The DISL (or nominee) and Designated Safeguarding Lead for the Day School and Sixth form, who is also the Deputy Designated Institutional Safeguarding Lead (DSL/DDISL), work closely together with the IT Team to meet the needs of the Institution and where relevant, ensure they attend online safety, including filtering and monitoring training and/or seek external specialist support.

25. For effective day-to-day management of the filtering and monitoring process, ArtsEd's DISL and the DSL/DDISL take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.

iii. The Designated Institutional Safeguarding Lead (DISL) has primary responsibility for:

a. acting as a named point of contact on all online safeguarding issues and liaising with other members of staff or other agencies, as appropriate.
b. working alongside other staff with designated safeguarding responsibilities (such as the Deputy Designated Safeguarding Lead and Designated Safeguarding Officers and Welfare) to ensure online safety is recognised as part of ArtsEd's safeguarding responsibilities and that a coordinated approach is implemented.
c. ensuring all members of staff receive regular, up-to-date and appropriate online safety training.
d. accessing regular and appropriate training and support and understanding the unique risks associated with online safety, and having the required up-to-date relevant knowledge required to keep learners (pupils and students) safe online.
e. accessing regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
f. keeping up to date with current research, legislation and trends regarding online safety, communicating this across the Institution, as appropriate.
g. ensuring positive online safety is promoted across ArtsEd and among the Institution's stakeholders through a variety of channels and approaches.
h. maintaining records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
i. monitoring online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
j. reporting online safety concerns, as appropriate, to SLB and the Board of Trustees.
k. working with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
l. meeting at least termly with the DST or nominee and the DSL/DDISL to discuss safeguarding and online safety, including filtering and monitoring.
m. The DISL may delegate part of their responsibilities to an appropriately trained member of staff.

iv. Designated Safeguarding Lead for the Day School and Sixth Form/Deputy Designated Institutional Safeguarding Lead (DSL/DDISL)

26. Reporting to the DISL, the DSL/DDISL lead the operational delivery of safeguarding and online safety in the Day School and Sixth Form, which could include overseeing and acting on:
    a. actions from filtering and monitoring reports and reporting updates to the 'Safeguarding and Welfare Operational Group' and 'Welfare, Safeguarding, Health and Safety Committee'.

b. acting as the DISL's nominee for safeguarding and online safety matters including concerns about filtering and monitoring.
c. acting on safeguarding concerns.
d. checking that the filtering and monitoring systems are effective.
e. raising online safety awareness and ensuring staff members are trained on online safety.
f. working alongside other staff with designated safeguarding responsibilities such as the (Deputy Designated Safeguarding Lead and Designated Safeguarding and Welfare Officers) to ensure online safety at ArtsEd.
g. working alongside PSHEE coordinators to ensure that Online Safety is a focus of all areas of the DSSF curriculum, and that staff reinforce Online Safety messages across their respective lessons. The Online Safety curriculum is broad, relevant and provides progression, and will be provided via the Institution's comprehensive PSHEEE curriculum and supported through the whole of the Day School's curriculum.

v. The IT Team has technical responsibility for:

a. maintaining filtering and monitoring systems.
b. carrying out scheduled and regular filtering and monitoring checks and reviewing and processing these in accordance with ArtsEd's requirements, ensuring compliance.
c. providing filtering and monitoring reports, including on learners (pupil and students) and staff, and details of device activities, providing these to the DISL and the DSL/DDISL.
d. completing actions following concerns or checks to systems and reporting updates to the DISL and DSL/DDISL.
e. identifying risks, including recording safeguarding concerns and notifying the DISL and DSL/DDISL promptly.
f. monitoring issues with devices ensuring monitoring systems are working to expected standards.
g. ensuring monitoring data is received in a format that staff can understand and that users are identifiable ensuring concerns can be traced back to an individual, including on guest accounts.
h. identifying technologies and techniques that allow users to avoid the filtering, such as VPNs and proxy services, and to block these.
i. ensuring that where mobile or app technologies are used, these have technical monitoring system added to devices to identify where filtering systems fail to identify inappropriate mobile or app content.

27. Where technical monitoring systems are used, the IT Team is responsible for ensuring a Data Protection Impact Assessment (DPIA) is undertaken and for reviewing the privacy notices of third-party providers. A DPIA template is available from the Information Commissioner's Office website. The DfE data protection toolkit also includes guidance on privacy notices and DPIAs.

28. The IT Team will undertake safeguarding training, including exercises focused on online safety, supporting the Executive to ensure ArtsEd meets the Broadband internet standards and Cyber security standards.

vi. ArtsEd's Staff Members

29. Safeguarding is everyone's responsibility and ArtsEd is aware that technical monitoring systems alone do not stop unsafe activities on a device or online. Therefore, ArtsEd's staff members are responsible for:
a. contributing to the development of online safety policies as well as reading and adhering to the online safety policy and acceptable use policies.

b. modelling good practice when using technology and maintaining a professional level of conduct in their personal use of technology, both on and off site. Staff should be aware that their online conduct outside of ArtsEd, including personal use of social media, could have an impact on their professional role and reputation.

c. undertaking safeguarding training including that directed towards online safety.

d. having an awareness of a range of online safety issues and how they may be experienced by the learners (pupils and students).

e. taking responsibility for the security of systems and the data they use or have access to.

f. providing effective supervision to learners (pupils and students), as appropriate.

g. taking steps to maintain awareness of how devices are being used by learners (pupils and students) and embedding online safety education in curriculum delivery, wherever possible.

h. being aware of reporting mechanisms for safeguarding including those relating to filtering, monitoring and technical concerns.

i. taking responsibility for their personal and professional development in this area.

j. reporting any safeguarding concerns to the DISL and/or DSL/DDISL promptly**. Staff members should report if:**

- they witness or suspect unsuitable material has been accessed.
- they can access unsuitable material.
- they are teaching topics which could create unusual activity on the filtering logs.
- there is failure in the software or abuse of the system.
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks.
- they notice abbreviations or misspellings that allow access to restricted materials.

- **ArtsEd's stakeholders**

vii. Learners (pupils and students)

30. ArtsEd's learners ((pupils and students) at a level that is appropriate to their individual age and ability) are responsible for:

a. engaging in age-appropriate online safety education opportunities.

b. contributing to the development of online safety policies.

c. reading, understanding and adhering to the IT acceptable use policies.

d. respecting the feelings and rights of others online and offline.

e. taking responsibility for keeping themselves and others safe online.

f. using any ArtsEd systems, such as learning platforms, and other network resources, safely and appropriately.

g. seeking help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

viii. Parents and carers of pupils and students under the age of 18

31. Parents and carers of ArtsEd's learners (pupils and students) who are under the age of 18 are responsible for:

a. reading and abiding by the Institution's IT acceptable use policies (including this 'Online Safety, Filtering and Monitoring Policy') which is made available to parents and carers by ArtsEd and encouraging their children to adhere to them.

b. engaging with internet safety awareness sessions, including the Online Safety newsletters or communications made available to parents and carers at parent evenings/meetings by the Institution and on ArtsEd's website.

c. contributing to the development of ArtsEd's online safety policies.
d. supporting ArtsEd's online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
e. acting as role models for safe and appropriate use of technology and social media.
f. identifying changes in behaviour that could indicate that their child is at risk of harm online.
g. seeking help and support from appropriate agencies if they or their child encounter risk or concerns online.
h. using any ArtsEd systems, such as the website and the learning environment (VLE), and other network resources, safely and appropriately.
i. taking responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

ix. Visitors including other service users (e.g., hirers)

32. All visitors such as, those attending a show or those who hire spaces from the Institution or access hired spaces are responsible for:
    a. ensuring they familiarise themselves with, and comply with, the Institution's IT acceptable use policies.
    b. acting appropriately and using ArtsEd's systems and networks safely.
    c. immediately seeking help from an ArtsEd staff member if there is a concern about online safety and promptly reporting any online concerns to safeguarding@artsed.co.uk

D. Filtering and Monitoring Review

i. Annual Filtering and Monitoring Review

33. ArtsEd reviews its filtering and monitoring provision at least once a year, or as required. For example, when a new safeguarding risk is identified, when there is a change in working practice such as 'Bring Your Own Device' and/or when new technology is introduced.

34. The review is conducted by the DISL, DSL/DDISL, the IT Team and the DST. The review reflects the Institution's operational organisation and considers:
    a. the risk profile of learners (pupils and students), including their age range, those with special educational needs and disability and those with English as an additional language (EAL).
    b. what the filtering system currently blocks or allows and why.
    c. any outside safeguarding influences, such as county lines.
    d. any relevant safeguarding reports.
    e. the digital resilience of learners (pupils and students).
    f. teaching requirements, for example, the RSE and PSHE curriculum (applicable to the DSSF only).
    g. the specific use of the chosen technologies, including 'Bring Your Own Device' (BYOD) and remote access.
    h. what related safeguarding or other technology policies are in place at ArtsEd.
    i. what checks are currently taking place and how resulting actions are handled.

35. The outcome of the annual review is recorded for reference, reported to the Welfare, Safeguarding, Health and Safety Committee as well as made available to appropriate persons entitled to inspect the information.

36. In order to assure the Board and the Executive that systems are working effectively and meeting safeguarding obligations, any additional checks or actions to filtering and monitoring arrangements will be informed by the review process noting any best practice, gaps and specific

needs of learners (pupils and students) and staff members. Additional checks and actions, where relevant, will also note the expectations on visitors and other service users such as hirers. The outcome of any review is used to inform:

a. related safeguarding or technology policies and procedures.
b. roles, responsibilities and training of staff members.
c. curriculum and learning opportunities.
d. procurement decisions.
e. how often and what is checked.
f. monitoring strategies.

ii. Checking Filtering Provisions

37. The checks of ArtsEd's filtering provision are completed and recorded as part of the Institution's filtering and monitoring review process. Such checks are undertaken from both a safeguarding and IT perspective.

38. When carrying out checks, the Institution ensures the filtering and monitoring systems in place have not changed or been deactivated and that checks include a range of:
   a. Institutionally-owned devices.
   b. departments in the Day School and Sixth Form, Higher Education, ArtsEd Extra and Hires including where these are off site.
   c. user groups, for example, teachers, lecturers, visiting staff, administrative staff, pupils, students and guests.

39. Logs which include the following are also kept:
   a. the dates that checks took place and the IT staff member that undertook the checking.
   b. what was tested or checked and any resulting actions.
   c. confirmation that filtering and monitoring systems work on new devices and services before releasing them to staff and pupils.
   d. that blocklists are reviewed and can be modified in line with changes to safeguarding risks.

40. The UK Safer Internet Centre offers guidance on establishing appropriate filtering and ArtsEd's filtering provider is a member of Internet Watch Foundation (IWF), is signed up to the Counter-Terrorism Internet Referral Unit list (CTIRU) and blocks access to illegal content including child sexual abuse material (CSAM).

iii. Checking Monitoring Provisions

41. Monitoring user activity on ArtsEd's devices is an important part of providing a safe environment for learners (pupils and students), staff members, visitors and relevant service users. Unlike filtering, it does not stop users from accessing material through internet searches or software but allows for reviewing user activity on institutional devices.

42. ArtsEd seeks to minimise safeguarding risks on internet connected devices and its monitoring of outputs informs the Institution's filtering and monitoring review. ArtsEd uses a variety of monitoring approaches such as:
   a. physically monitoring by watching the screens of users, where appropriate/relevant.
   b. network monitoring using log files of internet traffic and web access.
   c. individual device monitoring through software or third-party services.

43. Users are informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

44. The UK Safer Internet Centre has guidance for schools and colleges on establishing appropriate monitoring systems.

E. Safer Use of Technology

i. Use of personal devices, including mobile phones

45. ArtsEd recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents, carers and visitors, but technologies need to be used safely and appropriately.

ii. Staff Use of Personal Devices and Mobile Phones

46. Members of staff will refer to and adhere to the IT Acceptable Use policy and any other policy where the staff use of personal devices and mobile phones is referred to, such as the Staff Code of Conduct.

iii. Learners (pupils and students) Use of Personal Devices and Mobile Phones

47. ArtsEd set expectations for its learners (pupils and students) when using personal and mobile phones on its premises. The Institution educates learners (pupils and students) regarding the safe and appropriate use of personal devices and mobile phones, properly communicating awareness of boundaries and consequences. ArtsEd expects learners' personal devices and mobile phones to be kept in a secure place, switched off, kept out of sight during lessons and while moving between lessons. Mobile phones or personal devices are not allowed to be used by learners during lessons or formal educational time unless as part of an approved and directed curriculum-based activity and with consent from a member of staff. Please note that the use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.

48. The Day School and Sixth Form has a strict "no mobile phones" policy for Year 7 – 11 pupils. Mobile phones must be switched off and handed in during morning registration to the form tutor. The mobile phones are locked away in a secure area for the day and pupils can retrieve their mobile phones at the end of the school day.

49. Where any DSSF pupil needs to contact their parents or carers they will be allowed to use an ArtsEd telephone. Parents and carers of DSSF pupils are advised to contact their child via the relevant school's administrative office unless where agreed exceptions have been made by ArtsEd with the parent as it pertains to the child. The school administrator will only take emergency messages.

50. Mobile phones and personal devices must not be taken into examinations. Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

51. Where appropriate, and if a learner (pupil or student) breaches the policy, the phone or device will be confiscated and will be held in a secure place. Staff may confiscate a learner's (pupil or student) mobile phone or device if they believe it is being used to contravene an ArtsEd policy

such as Safeguarding Policy or Anti-Harassment and Bullying Policy or could contain youth-produced sexual imagery (sexting).

52. Any searches of mobile phones or personal devices will be carried out by the appropriate ArtsEd staff and will only be carried out in accordance with the Department for Education's 'Guidance for Searching, screening and confiscation in Schools' , ArtsEd's statutory obligations and in line with the relevant ArtsEd procedures. Searches will take place with the consent of the learner (pupil or student, where appropriate) or a parent or carer. Content may be deleted or requested to be deleted, if it contravenes ArtsEd's policies.

53. Mobile phones and devices that have been confiscated by ArtsEd will typically be released as appropriate to the learner (pupil or student), parents or carers at the end of the day.

54. Where there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

iv. Visitors' Use of Personal Devices and Mobile Phones

55. Parents, carers and visitors (including volunteers and hirers), when attending the Institution, must use their mobile phones and personal devices in accordance with ArtsEd's IT Acceptable Use Policy and other associated policies, such as the Anti-Harassment and Bullying policy and Safeguarding Policy.

56. ArtsEd will that ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors, including hirers, of the Institution's expectations as set out in ArtsEd's IT Acceptable Use Policy.

v. Officially-provided mobile phones and devices

57. Staff members must only use their ArtsEd work phone number and email address, where contact with learners (pupils and students), parents or carers is required. ArtsEd's mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by those members of staff to which these are assigned. ArtsEd's phones and devices must always be used in accordance with the IT Acceptable Use Policy and other relevant policies when issued.

F. Reporting and managing online safety incidents including filtering and monitoring concerns

58. Safeguarding is the responsibility of everyone, this includes reporting online safety concerns, such as breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content. Online safety issues, including filtering and monitoring concerns, should be reported promptly to the DISL and/or the DSL/DDISL by sending an email to safeguarding@artsed.co.uk or by calling 020 8987 6600. The DISL and/or the DSL/DDISL can also be notified in person. It is important that confidentiality is respected when reporting concerns and official procedures for reporting concerns are followed.

59. Once reported, the DISL and/or the DSL/DDISL will record the incident in line with ArtsEd's safeguarding policy and ensure that online safety concerns are escalated and reported to relevant internal departments and external agencies in line with the safeguarding harm thresholds and procedures.

60. Identified individuals who try to access unsuitable or illegal material who have been referred to the DISL and/or the DSL/DDISL (or deputies) may be referred by the DISL and/or the DSL/DDISL to appropriate staff and/or departments for additional support. If upon an assessment of the situation by the DISL and/or the DSL/DDISL (or deputies and/or nominee), other appropriate action may be taken including (the below is not an exhaustive list):
    a. asking the individual to undertake further training.
    b. referring the individual, where appropriate, to the relevant institutional disciplinary action and/or relevant ArtsEd policy.
    c. referring the individual to external agencies such as the police, Channel and/or the Local Authority Designated Officer (LADO). For example, where appropriate, ArtsEd's will follow its safeguarding procedures and inform the LADO should an alleged safeguarding incident, involving a child occur while an individual or organisation is using the Institution's premises or online facilities when running activities for children. **Please call the police on 999 if there is an immediate danger or risk of harm.**

61. Where appropriate and required, ArtsEd will inform parents and carers of online safety incidents or concerns involving their child.

62. ArtsEd, will debrief, identify lessons learnt and implement any policy or curriculum changes as required, following the completion of any investigations about safeguarding including those relating to online safety.

G. Procedures for Responding to Specific Online Incidents or Concerns

i. Online Sexual Violence and Sexual Harassment between Children

63. ArtsEd recognises that sexual violence and sexual harassment between children can take place online and that there is a potential for repeat victimisation in the future if abusive content continues to exist somewhere online. Examples may include non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation. It is further recognised that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

64. Where a report of online sexual violence and sexual harassment is made, the following steps set out below will be taken within the Institution.
    a. Immediately notify the DISL and/or DSL/DDISL and act in accordance with the Safeguarding and Anti-harassment and bullying policies.
    b. If content is contained on learners' electronic devices, they will be managed in accordance with the Department for Education's 'Guidance for Searching, screening and confiscation in Schools' advice.
    c. Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    d. Implement appropriate sanctions in accordance with relevant disciplinary policies.
    e. Inform parents and carers, if appropriate, about the incident and how it is being managed.
    f. If appropriate, make a referral to partner agencies, such as the LADO and/or the Police.

g. If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community. If a criminal offence has been committed, the DISL and/or DSL/DDISL (or deputy) will discuss this with police first to ensure that investigations are not compromised.

h. Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

ii. Youth Produced Sexual Imagery (“Sexting”)

65. ArtsEd recognises youth produced sexual imagery (known as “sexting”) as a safeguarding issue and the Institution will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using ArtsEd’s provided or personal equipment. All concerns will be reported to and dealt with by the DISL and/or DSL/DDISL (or nominee).

66. In managing such incidents, ArtsEd will follow the advice as set out in the non-statutory UK Council for Child Internet Safety Guidance ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’.

67. Anyone raising a concern about ‘Sexting’ MUST NOT view any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so. Where it is deemed necessary to do so, such an image will only be viewed by the DISL and/or DSL/DDISL and their justification for viewing the image will be clearly documented.

68. Content suspected to be an indecent image of a child (i.e., youth produced sexual imagery) **MUST NOT** be sent, shared or saved. Copies of content suspected to be an indecent image of a child (i.e., youth produced sexual imagery) **MUST NOT** be made by anyone at ArtsEd and no one at the Institution will allow or request learners or anyone else to do so.

69. Where a report of an incident involving the creation or distribution of youth produced sexual imagery is made, the following steps set out below will be taken within the Institution.

    a. Act in accordance with ArtsEd safeguarding policies and the relevant Local Authority Safeguarding procedures.

    b. Ensure the DISL and/or DSL/DDISL (or deputy DSLs) respond in line with the ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ guidance.

    c. Store the device securely. Where an indecent image has been taken or shared on the Institution’s network or devices, action will be taken to block access to all users and isolate the image.

    d. Carry out a risk assessment which considers any vulnerability of learners (pupils or students) involved, including carrying out relevant checks with other agencies.

    e. Inform parents and carers, if appropriate, about the incident and how it is being managed.

    f. Make a referral to Social Services (LADO) and/or the Police, as deemed appropriate in line with the ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ guidance.

    g. Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.

    h. Implement appropriate sanctions in accordance with the relevant disciplinary policies. However, care must be taken to ensure that victims are not further traumatise, where possible.

i. Consider the deletion of images in accordance with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance. Images will only be deleted once the DISL and/or DSL/DDISL (or deputy DSLs) has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.

j. Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

iii. Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

70. ArtsEd ensures that all members of its community are aware of online child sexual abuse, including exploitation and grooming, the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns. The Institution recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns must be reported to and dealt with by the DISL and/or DSL/DDISL.

71. ArtsEd will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or when using ArtsEd's provided or personal equipment.

72. Where a report of an incident involving online child sexual abuse and exploitation (including criminal exploitation) is made, the following steps set out below will be taken within the Institution.
    a. Act in accordance with ArtsEd safeguarding policies and the relevant Local Authority Safeguarding procedures.
    b. If appropriate, store any devices involved securely.
    c. Make a referral to Social Services (LADO), if required/appropriate and immediately inform the police via 101, or 999 if a child is at immediate risk.
    d. Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
    e. Inform parents/carers about the incident and how it is being managed.
    f. Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
    g. Review the handling of any incidents to ensure that best practice is implemented; the leadership team will review and update any management procedures, where necessary.
    h. If we are unclear whether a criminal offence has been committed, the DISL and/or DSL/DDISL will obtain advice immediately through the police by using 101.
    i. If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police using 101 by the DISL and/or DSL/DDISL unless where immediate concerns are raised. In such an instance call the police on 999.
    j. If learners at other external settings are believed to have been targeted, the DISL and/or DSL/DDISL (or deputy) will seek support from the Police first to ensure that potential investigations are not compromised.

iv. Indecent Images of Children (IIOC)

73. ArtsEd ensures that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) and will promptly respond to concerns regarding IIOC on all equipment (owned by ArtsEd and/or those personally owned), even if access took place off site.

74. The Institution works to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

75. Where a report of an incident involving accessing indecent images of a child/children is made, the following steps set out below will be taken within the institution.
    a. Act in accordance with our child protection policies and the relevant Local Authority Safeguarding procedures.
    b. Store any devices involved securely.
    c. Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), the police or the LADO.

76. Where it has been reported that a member of staff or a learner has been inadvertently exposed to indecent images of children, the following steps set out below will be taken.
    a. Ensure that the DISL and/or DSL/DDISL is informed.
    b. Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
    c. Ensure that any copies that exist of the image, for example in emails, are deleted.
    d. Report concerns, as appropriate to parents and carers.

77. Where it has been reported that indecent images of children have been found on an ArtsEd provided device, the following steps set out below will be taken.
    a. Ensure that the DISL and/or DSL/DDISL is informed.
    b. Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
    c. Ensure that any copies that exist of the image, for example in emails, are deleted.
    d. Inform the police via 101 (999 if there is an immediate risk of harm) and LADO.
    e. Only at the request of the police should copies of images be stored (securely, where no one else has access to them and delete all other copies).
    f. Report concerns, as appropriate, to parents and carers.

78. Where it has been reported that a member of staff is in possession of indecent images of children, the following steps set out below will be taken.
    a. In line with ArtsEd's Human Resources procedure ensure that the Principal and Headteacher (where it involves a DSSF staff and/or pupil) are informed immediately and without any delay.
    b. DSIL and/or DSL/DDISL to inform the LADO and other relevant organisations in accordance with ArtsEd's safeguarding policy.
    c. Quarantine any devices until police advice has been sought.

79. Where it is unclear if a criminal offence has been committed, the DISL and/or DSL/DDISL (or deputy) will obtain advice immediately from the Police using 101.

v. Cyberbullying

80. Cyberbullying, along with all other forms of bullying, will not be tolerated at ArtsEd. Full details of how we will respond to cyberbullying are set out in our anti-harassment and bullying policies. For more information, please see:
    - Anti-Bullying Policy for the Day School and Sixth Form

- Student Anti-Harassment and Bullying Policy for Higher Education Students
- Staff Anti-Harassment and Bullying Policy

vi. Online Hate

81. Online hate content, directed towards or posted by anyone at ArtsEd, will not be tolerated and will be responded to and investigated in line with existing policies, including anti-bullying and the Institution's disciplinary procedures. Reports of online hate can be made by sending an email to safeguarding@artsed.co.uk or using ArtsEd's Reporting Tool SpeakUp!

82. The Police will be contacted if a criminal offence is suspected. Where it is unclear if a criminal offence has been committed, the DISL and/or DSL/DDISL (or deputy) will obtain advice immediately from the Police using 101.

vii. Online Radicalisation and Extremism

83. ArtsEd takes all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. Where there is concern that a learner (pupil/student), staff member, trustee, parent or carer may be at risk of radicalisation online, the DISL and/or DSL/DDISL must be informed immediately. Report of this risk can be made to the Safeguarding team by sending an email to safeguarding@artsed.co.uk. Report can also be made in person to the DISL and/or DSL/DDISL (or deputy) or by calling 020 8987 6600.

84. Actions will be taken in line with the Institution's Safeguarding Policy and statutory requirements which may include a referral to Channel.

85. Where there is concern that a staff member may be at risk of online radicalisation, the Principal and Headteacher (where it involves a DSSF staff member) will be informed immediately, and action will be taken in line with the Safeguarding Policy and relevant Human Resources Policy.

viii. Cybercrime

86. Cybercrime incidents and offences will be responded to in line with the Safeguarding Policy and other relevant ArtsEd policies such as the IT Acceptable Use Policy and Staff Code of Conduct and disciplinary policies. ArtsEd will take seriously concerns that its learners (pupils and/or students) are involved, or at risk of becoming involved, in cybercrime regardless of where such takes place. Reports of incidents can be made to the Safeguarding Team by sending an email to safeguarding@artsed.co.uk. Reports can also be made in person to the DISL and/or DSL/DDISL (or deputy) or by calling 020 8987 6600.

Appendix A: Educating pupils about online safety.

All secondary schools have to teach ‘Relationships and sex education and health education in secondary schools’.

- **In Key Stage 3, pupils will be taught to:**

i. Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
ii. Recognise inappropriate content, contact and conduct, and know how to report concerns.

- **Pupils in Key Stage 4 will be taught:**

i. To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
ii. How to report a range of concerns.

- **By the end of secondary school, pupils will know:**

i. Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
ii. About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
iii. Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
iv. What to do and where to get support to report material or manage issues online
v. The impact of viewing harmful content.
vi. That specifically sexually explicit material (e.g., pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
vii. That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail.
viii. How information and data is generated, collected, shared and used online.
ix. How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.
x. How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.