ARTS EDUCATIONAL SCHOOLS

On-Line Safety Policy

Document Title	On-Line Safety Policy
Maintained by	SLT, Institutional Designated Safeguarding Lead, Finance Director, Holker
Owned by	Institutional Designated Safeguarding Lead
Institutional/Directorate Policy	Day School and Sixth Form
Approved by	DSSF Board
Last Reviewed	November 2026
Next Review	November 2027

ArtsEd Day School and Sixth Form
On-Line Safety Policy

1. INTRODUCTION

It is the duty of ArtsEd, and the Day School and Sixth Form in particular, to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for enhanced learning but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse and radicalisation and identity theft.

Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of ArtsEd include:

- Websites;
- Email and instant messaging;
- Blogs, forums and chat rooms;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites and online communities formed via games consoles;
- Instant messaging technology via SMS or social media sites;
- Video calls;
- Podcasting;
- Mobile applications;
- Virtual and augmented reality technology; and
- Artificial intelligence.

This policy, supported by the IT Acceptable Use Policy (for all staff, visitors and pupils), is implemented to protect the interests and safety of the whole School community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the other ArtsEd policies.

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At ArtsEd, we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **Content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

- **Contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- **Conduct**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

2. Scope of this Policy

This policy applies to all members of the ArtsEd community, including staff, pupils, parents and visitors, who have access to and are users of the ArtsEd IT systems. In this policy 'staff' includes teaching and non-teaching staff, trustees, and volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes on ArtsEd's premises.

Both this policy and the IT Acceptable Use (for all staff, visitors and pupils) cover fixed and mobile internet devices provided by the School (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto ArtsEd premises (personal laptops, tablets, smart phones, wearable tech etc).

In designing this policy, ArtsEd has considered the "*4Cs*" outlined in KCSIE (content, contact, conduct and commerce) as the key areas of risk. However, the School recognises that many pupils will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some pupils, may use mobile technology to facilitate child-on-child abuse, access inappropriate or harmful content or otherwise misuse mobile technology whilst at the School. The improper use of mobile technology by pupils, in or out of the School, will be dealt with under the School's POLICY: IT Acceptable Use; POLICY: Behaviour Management and/or POLICY: Child Protection & Safeguarding as is appropriate in the circumstances.

3. Roles and responsibilities

The Board of Trustees

The Board of Trustees has overall leadership responsibility for safeguarding as outlined in the policy on Child Protection & Safeguarding.

The Board of Trustees is responsible for the approval of this policy and for reviewing its effectiveness. The Board of Trustees will review this policy at least annually.

The Board of Trustees will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, to ensure that:

- all staff, in particular the DSL and SLT are adequately trained about online safety;
- all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise to escalate concerns when identified;
- staff are aware of the School procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the School.

The Principal and Executive Leadership Team

The Principal is responsible for the safety of the members of the ArtsEd community and this includes responsibility for online safety.

In particular, Executive Leadership Team are responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions, overseeing reports and ensuring staff are appropriately trained.

They will ensure that this policy is upheld by all members of ArtsEd community, and works with IT staff to achieve this. They will keep up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education (including KCSIE), ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

Any disclosure, report or suspicion of improper use of College IT or any issues with ArtsEd's filtering and monitoring system will be shared with the Executive Leadership Team as appropriate.

The Designated Safeguarding Lead (DSL)

The DSL takes the lead responsibility for Safeguarding and Child protection at ArtsEd. This includes a responsibility for online safety as well as the School's filtering and monitoring system.

The DSL will ensure that this policy is upheld at all times, working with the Principal and Executive Leadership Team and IT staff to achieve this. As such, in line with Child Protection & Safeguarding Policy, the DSL will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.

The DSL will work closely with ArtsEd's IT service providers to ensure that the ArtsEd's requirements for filtering and monitoring are met and enforced. The DSL will review filtering and monitoring reports and ensure that termly checks are properly made of the system:

IT staff

ArtsEd's IT staff, contracted with Holker, have a key role in maintaining a safe technical infrastructure at ArtsEd and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of ArtsEd's hardware system and its data. They are responsible for assisting in the training of ArtsEd's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the Safeguarding Team.

Teaching and support staff

All staff are required to sign the IT Acceptable Use before accessing ArtsEd's systems.

As with all issues of safety, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

All staff must read and understand this Online Safety Policy and enforce it in accordance with direction from the DSL and the Executive Leadership Team as appropriate.

Pupils

Pupils are responsible for using ArtsEd IT systems in accordance with the POLICY: IT Acceptable Use, and for letting staff know if they see IT systems being misused.

Parents and carers

Queen's College believes that it is essential for parents to be fully involved with promoting online safety both within and outside of College. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. ArtsEd will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with ArtsEd.

Parents are responsible for endorsing the IT Acceptable Use Policy.

4. Filtering and Monitoring

In general:

- ArtsEd aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of ArtsEd's safeguarding arrangements and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

- Staff, pupils, parents and visitors should be aware that ArtsEd's filtering and monitoring systems apply to all ArtsEd owned devices. Monitoring is throughSenso on ArtsEd Devices. Filtering is the Sophos firewall that logs and checks internet traffic; it is limited to devices that have connected to the ArtsEd network. Deliberate access, or an attempt to access, prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct and Behaviour Management, as appropriate.

- The Online Safety Coordinator will check once per term that the filtering and monitoring system are operating effectively – these checks must be recorded along with any appropriate action. From time to time the Safeguarding and/or Online Safety Trustee, the DSL and Online Safety coordinator will review the filtering and monitoring system,

looking at the records of the checks. Such a review should occur before the beginning of every new academic year, however such reviews should occur if:

  - there is a major safeguarding incident;
  - there is a change in working practices; or
  - if any new technology is introduced.

- ArtsEd's filtering system blocks internet access to harmful sites and inappropriate content. The filtering system will block access to child sexual abuse material, unlawful terrorist content, adult content as well as, but not limited to, the following: Cheating and Plagiarism, Gambling, Hacking, Hate Speech, Illegal Activities, Illegal Drugs . If there is a good educational reason why a particular website, application, or form of content should not be blocked a pupil should contact the relevant member of teaching staff, who will then contact the DSL for their consideration.
- ArtsEd will monitor the activity of all users across all of ArtsEd's devices or any device connected to ArtsEd's internet server allowing individuals to be identified. In line with ArtsEd's Privacy Notice, the DSL team and senior staff will monitor the logs daily. Any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSL immediately. Teaching staff should notify the DSL if they are teaching material which might generate unusual internet traffic activity.

Staff

- If any member of staff has any concern about the effectiveness of the filtering and monitoring system, they must report the matter to the DSL immediately in line with the Safeguarding and Child Protection Policy; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content. If any member of staff accidentally accesses prohibited or otherwise inappropriate content, they should proactively report the matter to the DSL.
- While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff should notify their head of their department if they believe that appropriate teaching materials are being blocked.

Pupils:

- Pupils must report any accidental access to materials of a violent or sexual nature or that are otherwise inappropriate to an appropriate teacher. Deliberate access to any inappropriate materials by a pupil will be dealt with under the policies. Pupils should be aware that all internet usage via ArtsEd's systems and its Wi-Fi network is monitored.
- Certain websites are automatically blocked by ArtsEd's filtering system. If this causes problems for ArtsEd work / research purposes, pupils should contact a member of staff for assistance.

5. Education and training

Staff

- As part of their induction, all new staff receive information on online safety, including ArtsEd's expectations, applicable roles and responsibilities regarding filtering and monitoring. This will include training on this Online Safety Policy.

- All teaching staff receive regular information and training on online safety issues in the form of staff training days and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety.
- All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following ArtsEd's Online-Safety procedures. These behaviours are summarised in the IT Acceptable Use. Understanding of this policy must be confirmed before first log on.
- Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of ArtsEd community. When pupils use School computers, staff should make sure children are fully aware of the agreement they are making to follow ArtsEd's IT guidelines.
- In accordance with Child Protection & Safeguarding Policy, if there is a safeguarding concern a report must be made by staff as soon as possible if any incident relating to online safety occurs and be provided directly to ArtsEd's DSL.

Pupils

- Online safety guidance will be given to pupils on a regular basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.
- The School provides opportunities to teach about online safety within a range of curriculum areas. Educating pupils on the dangers of technologies that may be encountered outside School will be covered via PSHE, by presentations in assemblies, as well as informally when opportunities arise.
- At age-appropriate levels, pupils are taught about their online safety responsibilities and to look after their own online safety. They are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to any member of staff at the School.
- Pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc).
- Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the School's Anti-Bullying Policy, which describes the preventative measures and the procedures that will be followed when the School discovers cases of bullying). Pupils should approach a Safeguarding Lead or online safety coordinator as well as parents, peers and other ArtsEd staff for advice or help if they experience problems when using the internet and related technologies.

Parents

- The School seeks to work closely with parents and guardians in promoting a culture of online safety. The School will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the School.

- The School recognises that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. The School therefore arranges regular discussion evenings for parents when an outside specialist advises about online safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

6. Use of College and personal devices

Staff

- ArtsEd devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.
- Staff at ArtsEd are permitted to bring in personal devices for their own use.
- Staff are referred to Staff Code of Conduct, and IT Acceptable Use for further guidance on the use of non-ArtsEd owned electronic devices for work purposes.
- Staff are not permitted to use their personal devices when taking images, videos or other recording of any pupil nor to have any images, videos or other recording of any pupil on their personal devices. Please read this in conjunction with policies on Child Protection & Safeguarding, IT Acceptable Use, Staff Code of Conduct, and Taking, Storing and Using Images of Children.

Pupils

- Pupils are responsible for their conduct when using School issued or their own devices. Any misuse of devices by pupils will be dealt with under the School's Behaviour Management Policy.
- The School recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents should arrange a meeting with the Head of Learning Development Department / the pupil's Head of Year to agree how the School can appropriately support such use. The Head of Learning Development Department / the pupil's Head of Year will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at School.

7. Online Communications

Staff

- Any digital communication between staff and pupils or parents/carers must be professional in tone and content. Personal telephone numbers, email addresses, or other contact details, may not be shared with pupils or parents / carers and recent alumni. The School ensures that staff have access to their work email address when offsite, for use as necessary on ArtsEd business.
- Staff must immediately report to the appropriate member of Executive Leadership Team, or DSL, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the IT Staff.

Pupils

- All pupils are issued with their own personal ArtsEd email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all School work assignments / research / projects. Pupils should be aware that email communications through ArtsEd network and School email addresses are monitored.

- There is strong monitoring, anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for School work / research purposes, pupils should contact their teacher for assistance.

- Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to the DSL, or another member of staff.

8. Use of Social Media

Staff

Staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of ArtsEd in accordance with Staff Code of Conduct.

Any online communications, whether by email, social media, private messaging or other, must not:

- place a child or young person at risk of, or cause, harm;
- bring ArtsEd into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or
- do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.
- otherwise breach Staff Code of Conduct or Child Protection & Safeguarding policy.

Any misuse of social media should be reported to the IT Department. Questions regarding the content or application of this policy should be directed to the SLT.

Pupils

- The School expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to an individual or others.

- The School takes misuse of technology by pupils very seriously and incidents will be dealt with under the Behaviour Management, Child Protection & Safeguarding, and Anti-Bullying, as appropriate.

9. Data protection

Please refer to the Data Protection and IT Acceptable Use Policy for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the School.

Staff and pupils are expected to save all data relating to their work to the ArtsEd system.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks or devices.

Staff should also be particularly vigilant about scam / phishing emails (and similar) which could seriously compromise ArtsEd's IT security and/or put at risk sensitive personal data (and other information) held by ArtsEd. If in any doubt, do not open a suspicious email or attachment and notify the IT Staff in accordance with Data Protection and IT Acceptable Use.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Data Controller.

10. Password security

The School recognises that secure passwords are a critical measure in protecting personal data, safeguarding systems, and preventing unauthorised access to school networks and online services.

All staff, Trustees, volunteers, and pupils (where appropriate) must use strong and unique passwords for school accounts. Passwords should be kept confidential and must never be shared with others, except where authorised systems provide secure account management arrangements. Users must not write passwords down in accessible locations or store them insecurely.

Staff must:

- Create passwords that meet the sShool's password complexity requirements;
- Use different passwords for school accounts and personal accounts;
- Change passwords immediately if they believe an account has been compromised;
- Enable multi-factor authentication (MFA) where this is available;
- Lock devices when unattended and log out of systems when access is no longer required; and
- Report any suspected security breach, phishing attempt, or unauthorised account access to the designated IT support team or senior leader without delay.

The School will implement appropriate technical controls, including password policies, account monitoring, and access management procedures, to help protect users and school information systems. Failure to comply with password security requirements may result in disciplinary action in accordance with the School's acceptable use policies.

Ultimately, all users are responsible for maintaining the security of their ArtsEd accounts and for protecting sensitive information from unauthorised access.

11. Safe use of digital and video images

- See the policy on Taking, Storing and Using Images of Children for further details.

12. Artificial Intelligence

ArtsEd recognises the increasing role of artificial intelligence (AI) in education and is committed to ensuring its safe, ethical and responsible use in line with Department for Education guidance. Any use of AI within ArtsEd must place the safety and wellbeing of pupils at the centre of decision making. See the Policy on AI for further details..

13. Misuse

ArtsEd will not tolerate illegal activities or activities that are in breach of the policies referred to above. Where appropriate ArtsEd will report illegal activity to the police and/or the local safeguarding partnerships. If the School discovers that a child or young person is at risk as a consequence of online activity they should report it to the DSL. The DSL then may seek assistance from CEOP, and/or its professional advisers as appropriate.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with ArtsEd's policies.

The School will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our policies on Anti-Bullying and Child Protection & Safeguarding.

14. Complaints

As with all issues of safety at ArtsEd, if a member of staff, a pupil or a parent has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed through the usual channels.

Incidents of or concerns around online safety will be recorded using My Concern. The DSL is immediately notified.