



ONLINE SAFETY POLICY

Last updated: September 2026	Next review: September 2027
Ratified by: Proprietor – Susi Earnshaw	

Individuals responsible for digital safety within school:

Proprietor: Susi Earnshaw

Headteacher: Megan McNamara

Designated Safeguarding Lead (DSL): Katherine Tyler

Deputy Designated Safeguarding Lead (DDSL): Melissa Gillespie

Filtering and Monitoring Systems: Securus Software

Contents

Introduction

Aims

Digital Technology at Susi Earnshaw Theatre School

Digital Technology and the curriculum

Online Safety

Filtering and Monitoring

Generative AI

Use of staff devices within school

Pupil device use

Appendix

References

Introduction

As stated by the UK Council for Internet Safety (2020), pupils are growing up in a complex world both online and offline. It is crucial that we support them to enjoy childhood and allow them to benefit safely from all the opportunities online can bring to them. However, it is also important they learn to balance these benefits and stay safe allowing them to make positive contributions to the online world.

At Susi Earnshaw Theatre School, we are committed to equipping our pupils with the skills and knowledge needed to flourish and succeed in an ever-changing digital society whilst maintaining the highest levels of safety and security, so our pupils are given the opportunity to recover and thrive after the adverse childhood experiences they have faced.

Aim

This policy aims to outline how, at SETS, we:

- Provide learning opportunities and promote digital safety across the school. - Have measures in place in line with statutory requirements in order to safeguard pupils and staff.
- Recognise the ever-changing digital world and how we can support our pupils to use this effectively, including AI.
- Support parents to provide the same level of guidance and work alongside them with the goal of supporting our young people.
- Are influenced by other policies within the school including but not limited to movies, video games, pornographic material and mobile phone use.

Digital Technology at Susi Earnshaw Theatre School

Digital technology is used across the school in many ways. Pupils are given opportunities to use laptops and iPads as learning tools, to research information, as intervention and support tools, and to be presented learning opportunities in different ways. Depending on individual needs, pupils may use apps, websites, windows and other software, and can be presented work through images, videos, links and publications.

Teachers are supported to use a range of digital tools to provide different learning opportunities and can access a range of different websites and resources including doodle and Kahoot.

We follow the guidelines of age-related ratings and PEGI as well as determining the appropriateness of all media used for our pupils depending on the needs of the curriculum.

Digital Technology and The Curriculum

Our curriculum recognises that anyone can be vulnerable online and that this can fluctuate. It is important at all times that we consider how we tailor learning to make sure everyone receives the education they need and deserve without causing trauma or harm.

All pupils participate in online safety lessons within PSHCE and are reminded of the ICT use agreement they sign at the beginning of each year (Appendix A).

The curriculum will provide opportunities for pupils to develop knowledge and skills including:

- safe use of laptops, tablets and other digital devices;
- safe and effective internet searching;
- evaluating the reliability of online information;
- misinformation and disinformation;
- recognising fake or manipulated content;
- passwords and account security;
- protecting personal information;
- digital footprints and online reputation;
- privacy and consent;
- online relationships;
- respectful communication;
- cyberbullying;
- online harassment;
- social-media safety;
- online grooming and exploitation;
- pornography and harmful sexual content;
- making or sharing nudes and semi-nudes;
- AI-generated and digitally manipulated images;
- deepfakes and other deceptive content;
- online scams, phishing and financial exploitation;
- online gambling and commercial risks;
- radicalisation and extremist content;
- misogynistic and other harmful online content;
- digital resilience;
- reporting concerns and seeking help; and
- responsible and safe use of artificial intelligence.

KCSIE 2026 specifically identifies online harms including image sharing, deepfakes, pornography and misogynistic influencers as issues that should be addressed through preventative education at an age-appropriate stage.

Online-safety education will be integrated into relevant curriculum areas and safeguarding education rather than treated solely as an ICT issue.

Where appropriate, the school will use trusted resources from organisations including the Department for Education, UK Council for Internet Safety, UK Safer Internet Centre, SWGfL, NSPCC, CEOP and other appropriately vetted sources.

Online Safety

Online safety is a vital element of digital learning. Pupils need to develop the knowledge and skills required to keep themselves and others safe when using online platforms. Online safety is a priority across the school. Pupils are taught about key issues such as protecting personal information, cyberbullying, and the safe and responsible use of social media.

Teachers regularly discuss and reinforce online safety during all digital learning opportunities and promote internet safety through class-based workshops and other learning activities. Online and cyber safety, along with digital resilience, are further strengthened through whole-school participation in Safer Internet Day.

Any online safety concerns are recorded and shared with the senior leadership team, and others as required.

Filtering and Monitoring at Susi Earnshaw Theatre School

This applies to all employees of Susi Earnshaw Theatre Projects Ltd and aims to ensure that effective safeguarding when children are using the internet is at the heart of all decision-making. We have developed our policies and procedures and delivered guidance and training to ensure that we are prepared to safeguard our children while they are using the IT equipment we provide in our school. To provide this guidance, we have consulted DfE standards for filtering and monitoring and ensured compliance with Keeping Children Safe in Education (KCSiE, 2025).

This section includes the expectations and responsibilities for our school around effective filtering and monitoring.

Our approach to Filtering and Monitoring

When considering filtering and monitoring, filtering is used to provide a proactive and preventative measure that prevents staff and pupils from accessing inappropriate material by identifying and blocking content. Monitoring is a reactive measure and therefore does not block staff and pupils from accessing material but can observe inappropriate activity, allowing us to record this and act.

KCSiE (2026) refers to the 4 Cs that must be considered and appropriately planned for when filtering and monitoring pupil and staff activities online:

- a. **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. RSHE guidance for 2026, published in summer 2025, introduces new content concerns, including:

- i) Online scams – for example, ‘sextortion’, where individuals are blackmailed using sexually explicit material.
- ii) AI-related risks, including the malicious use of deep fakes and chatbots.
- iii) Fake or AI-generated social media profiles.

Susi Earnshaw Theatre will include these in its PSHCE provision to help pupils learn how to recognise this kind of deception and sharpen their digital literacy.

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

As stated in DfE Filtering & Monitoring Standards, we have ensured that we have: ●

Identified and assigned roles and responsibilities to manage filtering and monitoring systems.

- Ensured the review of our filtering and monitoring provision annually.
- Blocked harmful and inappropriate content without unreasonably impacting teaching and learning.
- Developed effective monitoring strategies to meet the safeguarding needs of pupils and staff.

Roles and responsibilities within Filtering and Monitoring

The roles and responsibilities to manage filtering and monitoring systems are clearly identified to allow everyone to work together to safeguard pupils and staff effectively. Furthermore, the clarity ensures professional expertise is used to make informed decisions. As head teacher, Susi Earnshaw holds overall responsibility for filtering and monitoring and assuring the standards are met.

DSL and Deputy DSLs

As detailed in KCSIE (2026), our DSL leads on safeguarding and online safety. Specific duties include:

- checking relevant reports
- responding to safeguarding concerns identified by filtering and monitoring

- assuring that filtering and monitoring systems are working effectively and reviewed regularly

SLT Responsibilities

The SLT is responsible for:

- buying filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of our provision
- overseeing reports

They are also responsible for making sure that all staff understand their role and are appropriately trained to follow policies, processes and procedures and act on reports and concerns.

Responsibilities also include:

- Supporting buying systems and identifying risks.
- Supporting reviews.
- Carrying out checks including identifying school devices and ensuring software is applied.
- Ensuring all staff are up to date with online safeguarding procedures and training (alongside training manager).
- Provide half termly monitoring information and data including any incidents. ● Ensure internet filtering and monitoring logs are up to date and provide new ones if necessary.
- Ensure users are identifiable to the school, so concerns can be traced back to individuals (Laptops are all assigned a number to be identifiable)

Third-Party IT Support provided by Securus (Filtering system)

Responsibilities include:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or system checks

Review of filtering and monitoring annually

As part of the annual safeguarding review, the DSL with the support from the DDSL and SLT, completes a Filtering and Monitoring review to ensure the needs of the children and staff are being appropriately met. This information can be requested and made available to anyone who is entitled to inspect it.

The annual review is carried out in line with the DfE Meeting Digital and Technology Standards in School and Colleges document. This annual review of our approach considers and reflects the

risks that our pupils face, both collectively as technology and apps change, and individually in terms of their own circumstances.

ONLINE SAFETY POLICY Page 7 of 15

A review will take place, as a minimum annually, or if:

- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD
- new technology is introduced, such as new devices
- major software updates occur
- there are changes to the technical configuration of the network and devices

The school will complete a formal review of filtering and monitoring at least once during every academic year.

The review will be led by the SLT member responsible for filtering and monitoring, with support from the DSL and IT support/provider.

The review will consider:

- whether filtering is operating effectively;
- whether monitoring is operating effectively;
- all internet-connected school devices;
- relevant locations and networks;
- mobile and portable devices;
- emerging technologies;
- generative AI;
- age and vulnerability of pupils;
- SEND and accessibility considerations;
- incidents and alerts;
- false positives;
- over-blocking;
- under-blocking;
- staff understanding;
- reporting and escalation arrangements;
- supplier performance;
- technical configuration;
- user identification;
- safeguarding outcomes; and
- whether further controls or training are required.

The school will retain a written record of the review, findings, actions and responsible persons.

A review will also be undertaken when:

- a safeguarding concern identifies a weakness;

- a new technology or significant application is introduced;
- there is a major change to the network;
- remote access arrangements change;
- BYOD arrangements change;
- significant software or configuration changes occur; or

ONLINE SAFETY POLICY Page 8 of 15

- there is another material change to the school's risk profile.

Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.

The filtering software used, Securus, blocks access to harmful sites and alerts 2 staff members via email to ensure any action required is effectively managed. DSLs and School leaders are responsible for ensuring that there is an appropriate response to the alert. This may include assigning it to a particular staff member to review and investigate and taking necessary steps in accordance with the Safeguarding and/or Behaviour Policy.

Securus software provides proactive digital safeguarding by monitoring device and network activity to identify inappropriate content, such as self-harm, bullying, or extremism. It takes screenshots of incidents, alerting staff to risks, and allows for both self-managed monitoring or a Full Managed Service (Securus FMS).

Installation:

Securus software installed onto the devices or the network (or both). Designated staff details are loaded with contact details for alerts. '

Monitoring:

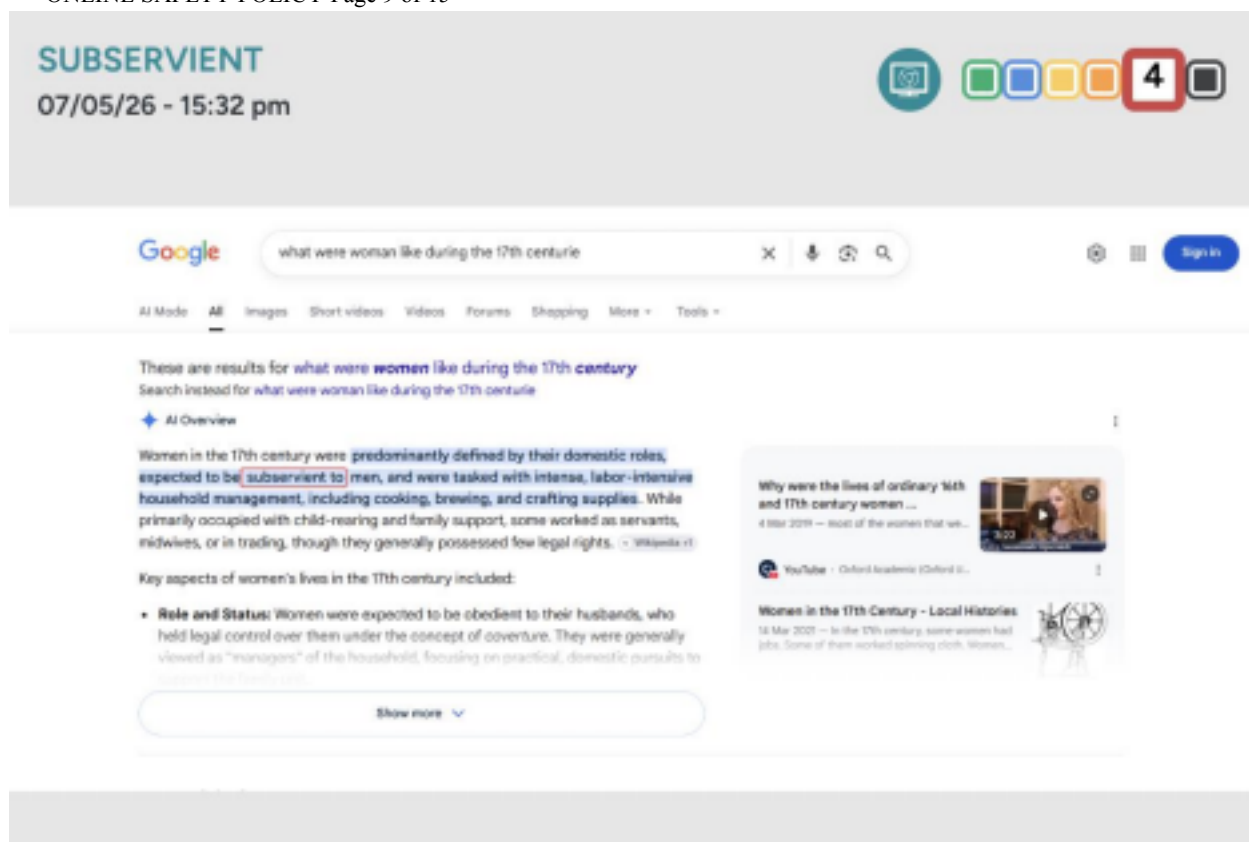
Designated staff monitor activity daily for incidents of concern. Incident Captures' are graded by severity. Severity 1 is low risk, up to Severity 5 being the highest risk.

Detection

When a capture of concern is detected, the Susi Earnshaw Safeguarding team will analyse and determine the level of risk from the detailed evidence and ascertain whether it is a false/positive capture or one of greater concern.

Alerts

Severity 4 & 5 captures generate email alerts that are immediately sent to our designated staff for our attention and urgent action. For Severity 5 captures, the school will receive a telephone call which is also backed up by an SMS message.



The DfE's filtering and monitoring standard was updated during 2026, including to reflect generative-AI risks.

Generative Artificial Intelligence (AI)

When discussing Generative Artificial Intelligence, It refers to technology that can be used to create new content based on large volumes of data that models have been trained on a variety of

sources (DofE 2025).

As stated by the DofE (2025), Generative AI presents exciting opportunities to improve people's lives. If used safely, effectively and with the right infrastructure in place, AI can support every child and young person, regardless of their background, to achieve at school and college and develop the knowledge and skills they need for life. As a school, we support teachers to use AI to support them to do what they do best and encourage its use to reduce administrative burdens that staff face on a day-to-day basis.

The evidence of Generative AI and its benefits and risks to pupils using it is still emerging and we must ensure that we remain informed by research and case studies. It is important whilst teaching pupils that the risks alongside the opportunities and benefits as well as each pupil's experiences and understanding are all considered and inform our judgement.

ONLINE SAFETY POLICY Page 10 of 15

At the time of writing this policy, all pupils are taught what AI is and the risks and benefits to individuals and society; however, it is not used by pupils. This will continue until we can ensure we can safeguard our pupils effectively in accordance with the current guidance.

DfE guidance on Generative AI (August 2025) identifies product safety expectations for edtech developers and suppliers to schools. This guidance will inform our decisions about what can safely be introduced to Susi Earnshaw Theatre pupils and when.

Use of staff devices within school

Susi Earnshaw Theatre School permits the use of employees using their own personal mobile devices for work purposes, including email, and file sharing.

Important and school specific information includes:

- Any personal device must contain a level of security in line with our existing IT infrastructure; this will include passcode protection and automatic locking when idle.
- The school accepts no responsibility for any loss or damage to personal devices that are the result of employee failure to observe rules, procedures or instruction, or, as a result of negligent behaviour.
- The school may need to apply security policies to staff devices which will protect the school's information held on such a device. We expect staff to accept any updates pushed to their device by the school.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of school and personal data due to operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

Photography and video recording of Pupils in Susi Earnshaw Theatre School

At Susi Earnshaw Theatre School we are committed to ensuring the safety and promoting the

welfare of the children in our care and we expect staff to share the same commitment.

It is the policy of the school that photography or video recording of pupils, their work, or anything else which could identify a pupil is undertaken by school staff only on devices owned by Susi Earnshaw Theatre School. Photographs and video recording must be taken solely for the purpose of recording a child or a group of children participating in activities or celebrating their achievements as an effective form of recording their ability and progress.

Pupil Device Use

This section outlines the expectations regarding the use of mobile phones and personal electronic devices within the school environment. The is designed to support teaching and learning,

ONLINE SAFETY POLICY Page 11 of 15

safeguard students, promote positive behaviour, and protect all members of the school community from online harm, bullying, harassment, and misuse of technology.

Pupils are not permitted access to personal mobile phones or personal electronic devices during the school day.

- Devices must be switched off and stored securely at the school reception at the beginning of the school day.
- Mobile phones must not be seen, heard, or used on school premises during the school day unless expressly authorised by a member of staff.
- Students must not use mobile phones during lessons, tutor time, social times, movement around school, or enrichment activities.
- Any unauthorised use may result in confiscation and further sanctions in line with the school behaviour policy.

The school recognises that many children now have unlimited and unrestricted access to the internet through mobile phone networks, including 3G, 4G, and 5G services. This access can expose children to harmful content and unsafe online behaviours.

Students must not:

- Use digital devices to sexually harass, intimidate, bully, or exploit other students. • Take, share, possess, or request indecent or sexually explicit images or videos. • Share nude or semi-nude images consensually or non-consensually.
- Access, upload, view, or distribute pornography or other harmful online material. • Use mobile data services to bypass school safeguarding and filtering systems. • Record or photograph students or staff without permission.

Any incident involving online abuse, sexual harassment, indecent imagery, pornography, or harmful content will be treated as a safeguarding matter and dealt with in line with statutory guidance and school safeguarding procedures.

Safeguarding and Online Safety

The school recognises that many young people now have unlimited and unrestricted access to the

internet through personal mobile devices and mobile phone networks. Such access can expose students to harmful, illegal, or inappropriate content and behaviour.

Students are expected to:

- Use technology safely, legally, and ethically.
- Respect the privacy, dignity, and safety of others online and offline.
- Report harmful or concerning online behaviour to staff immediately.

Any incident involving sexual harassment, online abuse, indecent images, pornography, exploitation, or harmful content will be treated seriously and managed in line with safeguarding procedures, statutory guidance, and, where necessary, police involvement.

Confiscation and Searches

Where there is reasonable concern that a device contains prohibited, harmful, or illegal material, the school reserves the right to confiscate the device and act in accordance with safeguarding and behaviour procedures.

Sanctions

Failure to comply with this policy may result in:

- Confiscation of the device.
- Parental or carer contact.
- Loss of permission to use personal devices in school.
- Detentions, isolation, suspension, or other behaviour sanctions. •

Referral to safeguarding leads or external agencies where appropriate.

ICT & ONLINE SAFETY AGREEMENT

Name: _____

Year Group: _____

Date: _____

This agreement supports the safeguarding duties set out in Keeping Children Safe in Education 2025 (KCSIE) and explains how students must behave when using ICT and online systems.

When I use the iPads or Laptops, I agree to be responsible, respectful, and safe.

I agree that I will:

- Be kind and respectful online and never take part in cyberbullying.
- Only use the internet or devices when a member of staff has given permission. • Only communicate online with people I know or who have been approved by an adult. • Never open emails, messages or links from unknown sources without checking with staff.
- Never share personal information such as my address, phone number or school details. • Never arrange to meet anyone I have spoken to online.
- Only use cameras, webcams or microphones with staff permission.
- Tell a member of staff immediately if I feel unsafe or see something inappropriate online. • Never try to access age inappropriate or unsuitable content.
- Never make online or in app purchases using school devices.
- Not attempt to bypass filters, firewalls or monitoring systems.
- Not download, upload or install files or software without permission.
- Never contact or befriend staff on social media.

I understand that my online activity may be monitored to keep me and others safe and that failure to follow this agreement may result in sanctions.

Student Signature: _____

Date: _____

I understand that being able to use the devices during class time is a privilege; if I chose not to follow the above expectations, I am aware I may not be able to use the devices.