Sylvia Young Theatre School

Internet Safety Policy
(incl. social media and cyberbullying)

Policy responsibility:	Menifa Williams Assistant Headteacher - Safeguarding (DSL)
Date reviewed:	6th September 2025
Reviewed	Annually

INTERNET SAFETY POLICY (including Social Media and Cyberbullying)

Internet safety is addressed in a variety of other school documents listed below, and referred to in other sections of this policy, that need to be read alongside this policy

1. **Acceptable Use Policy (computers, the internet and e-mail) –** All new students, parents and carers are provided with this policy and a form to be signed as part of their pre-admission pack.
2. **Staff Code of Conduct (section 3 of the Sylvia Young Theatre School Safeguarding Policy) –** before starting work at the Sylvia Young Theatre School all staff sign agreement to the staff code of conduct which covers appropriate and acceptable use of Social Media and the internet in sections entitled 'Social Media and Communication' and 'Internet Use'.
3. **Safeguarding & Child protection policy –** In addition to the section on staff code of conduct, many other sections of the safeguarding policy are also relevant to on-line safety.
4. **Anti-Bullying Policy –** any instances of **cyber bullying** will be dealt with according to the procedures set out in our Anti-Bullying Policy. The school follows the guidelines in the DfE document 'Cyberbullying: Advice for headteachers and school staff' in dealing with instances of cyberbullying: Cyberbullying: Advice for headteachers and school staff - GOV.UK
5. **Behaviour Policy –** the school rules section of the behaviour policy contains guidelines on mobile phone usage and safety / security, and on photos and videos on the internet. These sections are of the policy reviewed and updated regularly in line with the constant developments in the use of technology and social media.
6. **Rewards and Sanctions policy –** appropriate school sanctions will be used for infringements of school rules on the safe use of the internet. For serious breaches of on-line safety which have safeguarding implications, specific guidance will be sought, and followed, from the DfE document 'Keeping Children Safe in Education (KCSIE)'
7. **PSHE Policy –** the PSHE policy sets out how PSHE is covered across the whole curriculum, through individual subjects, assemblies, form time, visiting speakers and trips and visits.

- Personal Education includes helping students to stay safe and recognise dangers;
- Social, (Moral and Cultural) Education includes learning how to recognise and avoid exploitation, bullying and abuse.
- Safety on-line is frequently addressed in assemblies & form time with information & discussion in relation to issues arising either in school or nationally. Assemblies on the benefits and dangers of social media and on anti-bullying have been presented by form groups. External speakers have included the police, representatives from 'Transport for London', and volunteers from 'the Samaritans' and 'Body Gossip' all covering different aspects of the use and dangers of technology and social media, and the effects of cyberbullying. Visits have included trips to the Sutton Life Centre addressing personal safety, safety on-line & cyber-bullying)

8. **Curriculum Policy –** Internet safety and social media issues are addressed through ICT and other subject areas in the curriculum. Use is made of the websites CEOP Education and www.saferinternet.org.uk

   In particular:

- Students are made aware of dangers on the internet: the risks when using social network sites, the incidence of cyberbullying and the risk in giving personal details. They are also made aware of what actions to take if they think their personal liberties have been infringed.

- Students are encouraged to be aware of the benefits of new technology and its inherent problems. They are made aware of the Data Protection Act and their rights as citizens about data held on them

- Students are encouraged to be aware of the pitfalls of the internet – that it is a global, uncensored medium and all data should be treated with care. They are also taught to be aware of security issues associated with services such as auction sites/banking/shopping.

- Students are made aware through PSHE lessons of online safeguarding risks from Content, Contact, Conduct and Commerce and also the risks from misinformation, disinformation, and conspiracy theories

- Students are made aware of the Health and Safety legislation and guidelines when using information and communication technology.

ROLES AND RESPONSIBILITIES

Roles and responsibilities for on-line safety as part of the school's wider safeguarding strategy and how this links with other safeguarding policies

The oversight of online safety in the school is the responsibility of the Assistant Headteacher (DSL), and the Senior Management team and the Directors.

Individual subject teachers are responsible for educating students in online safety, and keeping an overview of their activity as far as is practically possible, when using technology in their lessons.

Links with other policies are as detailed in the list of documents at the beginning of this policy

GUIDANCE

Guidance on the use of technology in the classroom and beyond for all users, including staff, students and visitors including permissions/restrictions and agreed sanctions

Guidance is detailed in the following documents & policies from the list at the beginning of this policy:

- Acceptable Use Policy
- Staff Code of Conduct
- Behaviour Policy (including Rewards and Sanctions)
- Exclusion Policy
- Anti-Bullying Policy

The school allows students to bring mobile phones to school for several reasons including personal safety when travelling, being able to contact their parents/carers if they are delayed due to auditions or vocational work. However, student mobile phones are not allowed to be used throughout the school day.
We recognise that our filtering / blocking systems cannot restrict what the students have access to on their own devices over public WiFi, 4G & 5G
We address this issue by collecting the phones at the start of each day, educating the students about safe and appropriate internet use, and by raising parental awareness of the issue.
Parents' awareness of the issue will be raised through newsletters and our school website. We advise that parents/carers should install parental controls on their child's individual devices if they want to restrict their access. There is useful advice for parents/carers about to do this on the website 'internet matters' in the section 'set controls' Internet Matters Parental Controls

TECHNICAL PROVISIONS AND SAFEGUARDING

Technical provision/infrastructure and the safeguards in place to filter and monitor inappropriate content and alert the school to safeguarding issues

The school uses the security tools listed below, the correct functioning of which is the responsibility of the member of staff responsible for ICT maintenance.

In addition, the academic ICT teacher is trained in the use of **Netsupport Classroom Cloud** software.

1. Infrastructure Protection – Workstations and Servers - Server and client connections protection against intrusion from third parties and includes antivirus and anti malware software.

PC's - Microsoft Essentials and Microsoft Defender software protection from Microsoft which is controlled with regular planned update releases. Premium Avast Security software protection from Avast which is controlled with regular centralised released updates. Malwarebytes - Malwarebytes provides advanced protection against malware, ransomware, malicious websites, and other advanced online threats that have made traditional antivirus ineffective.

Macs - Premium Avast Security software protection from Avast which is controlled with regular centralised released updates. Malwarebytes - Malwarebytes provides advanced protection against malware, ransomware, malicious websites, and other advanced online threats that have made traditional antivirus ineffective. In addition to this all machines are locked down further via JAMF MDM (mobile device management) software.

2. NetSupport Classroom Cloud Safeguarding Software

https://classroom.cloud/best-school-software/

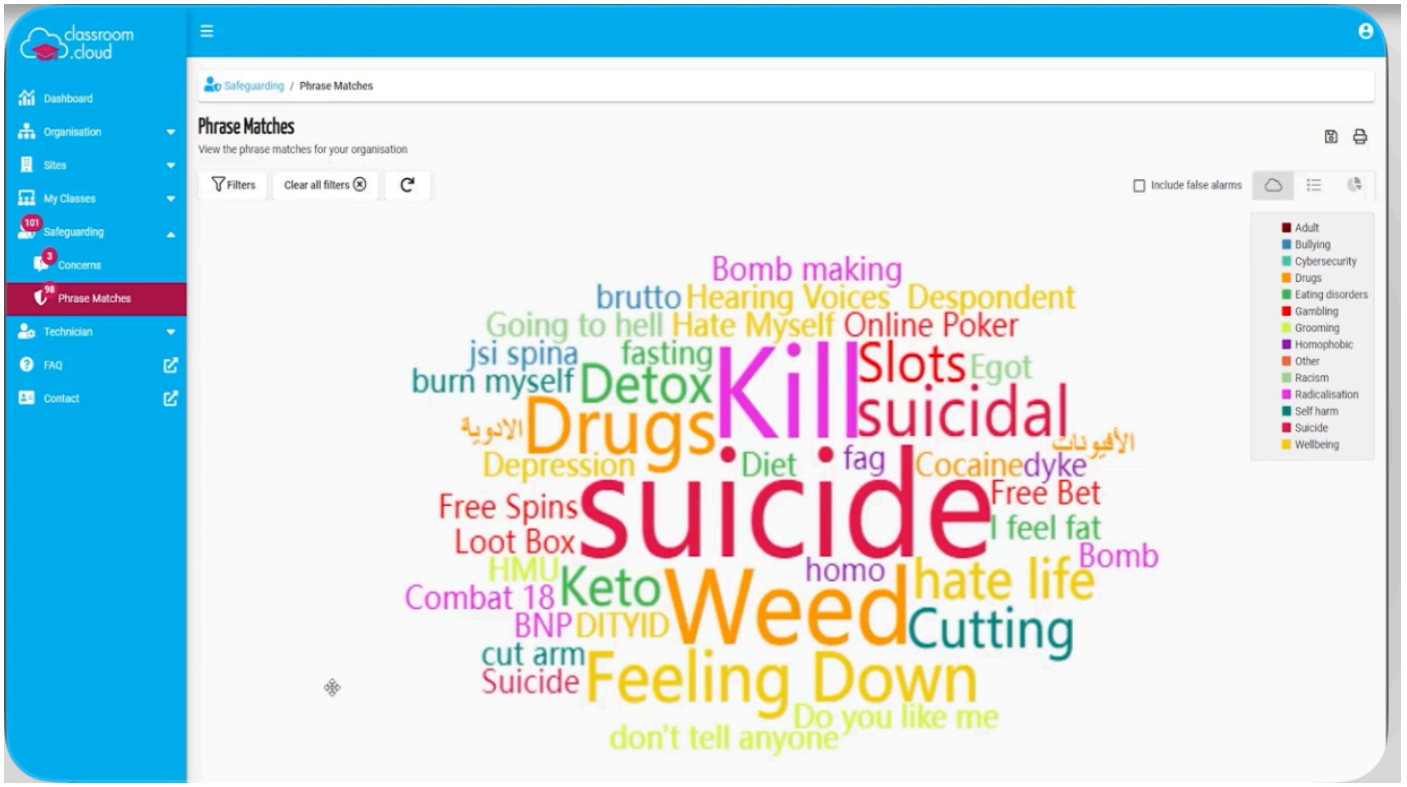
classroom.cloud - The highlights

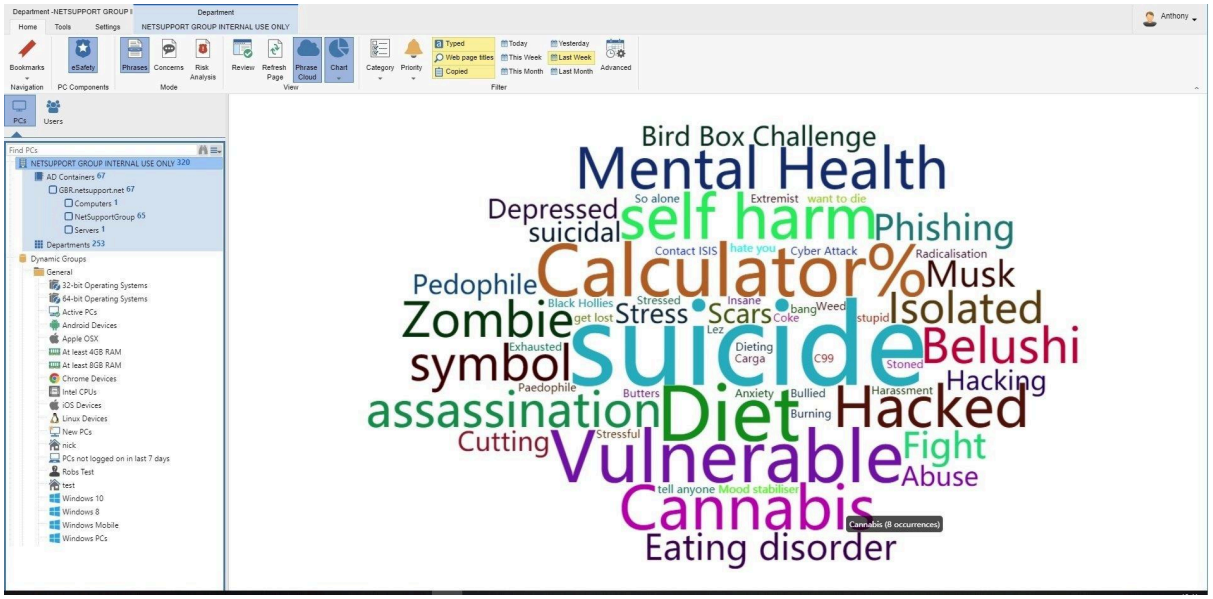
NetSupport Classroom Cloud provides a range of eSafety features. This includes both Internet Monitoring and restrictions to prevent access to inappropriate websites; disabling webcams on classroom devices; monitoring access to content on memory sticks; triggering Alerts when violations occur − through to the enforcement of acceptable usage policies.

NetSupport Classroom Cloud's Keyword and Phrase Monitoring feature provides insight into and alerts from any activity by a student that might suggest they are engaged in activity that would place them at risk. The details/context of triggered words can be reviewed, with the results (available as a log, screenshot of the screen, webcam image of the user, or a screen recording, according to severity level and which of these the school activates – features are not available for

devices used at home), forwarded to a colleague to follow up on, if required. The data captured is securely stored and forwarded to our safeguarding leads to instantly review the alert.

A full explanation and definition of each keyword is also given to help staff understand the potential risk to the student, plus the new contextual intelligence-based risk index creates a numerical risk index score for each event based on sophisticated contextual AI risk analysis. This allows staff to view high-risk events and vulnerable students with ease. Staff can also see the broader context of a student's activity from a detailed summary of their internet and application use (which can also be controlled) that is available for any selected period of time. Age appropriate internet controls can also be added using the Profiles. In addition, vulnerable students can be flagged and tracked as an extra layer of support, and a 'history of concerns' is available for each student.





The Azure-hosted safeguarding Cloud Console stores data to allow Safeguarding Leads to view triggered safeguarding keywords, new contextual intelligence-based risk alerts, reported concerns by a student and the trending topics word cloud on the go. The new cloud module also includes a smartphone optimised user interface to allow safeguarding staff to quickly search for a specific student and review any recent alerts or concerns.

NetSupport Classroom Cloud also enables Students to access online support resources – covering topics such as FGM, drug addiction, grooming and bullying – all from the Classroom Cloud safeguarding icon on their computer. Students can also report their concerns in confidence to a trusted member of staff via the 'Report a Concern' option.

Students can share their problem by sending a message, screenshots or documents to a member of staff they trust, then NetSupport Classroom Cloud will track the concern, any notes made, and even alert a Safeguarding Administrator if the intended member of staff has not responded within a certain amount of time. Concerns can be re- assigned to another Safeguarding Lead if for example the member of staff was on holiday. Teachers can also do the same in situations where they are verbally told of a student's concern. They can log the concern via the 'Add concern' button on the safeguarding ribbon.

At Sylvia Young Theatre School, the 'captures' from Classroom Cloud are emailed instantly to the network administrators and safeguarding team. The Network Administrators are not responsible for reviewing the content of captures, other than those of a technical nature such as hacking, but would alert the DSL immediately to any captures that were very obviously of a serious nature or that could be a safeguarding concern. The captures are also reviewed throughout the day to identify any individual captures of concern, and to look for any trends. The ICT co-ordinator passes weekly reports on to the DSL, who reviews them weekly. The DSL alerts the Headteacher and Safeguarding Director if there are any serious concerns.

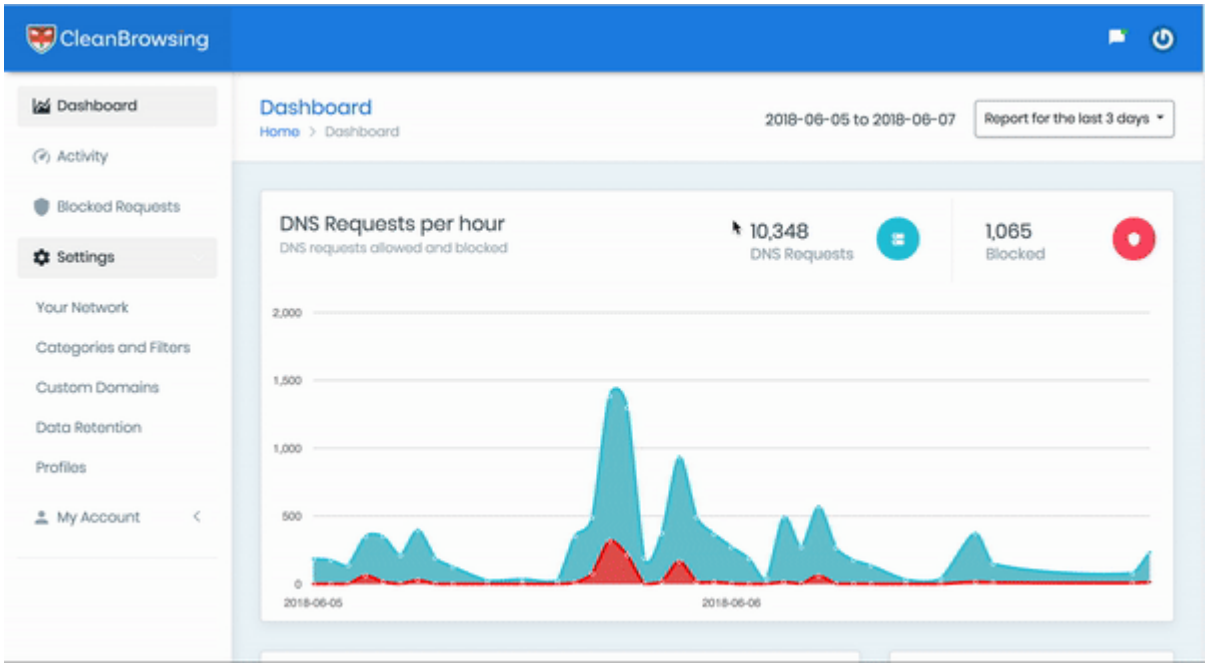
3. Google G-Suite / formerly Google Apps for Education - Using Group Policy Management

4. CleanBrowsing - premium DNS based Internet filter set up on all machines

CleanBrowsing is a premium DNS-based content filter, parental control and Safe Search enforcement service. It gives us advanced visibility and control of our network and the sites being visited. It is widely used by organizations of all sizes (e.g., schools, enterprises, non-profits) all over the world. CleanBrowsing essentially gives us the control to decide what is acceptable or not on our network.

CleanBrowsing provides protection measures that block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors). CleanBrowsing can also be used to monitor the online activities of minors. This include blocklists from the **Internet Watch Foundation** and the **Counter Terrorism Internet Referral Unit**
Internet Watch Foundation
CleanBrowsing | IWF Membership

Counter Terrorism Internet Referral Unit
[23+ CleanBrowsing Predefined Filters]



In addition to explicit blocking of obscene or explicit content, CleanBrowsing enables us to control student access through a series of default filters (total of 14), custom application blocking, and an engine that allows us to define our own blocking categories.

Default filters allow us to control categories of content such as: Social media, Gambling, Violence, Torrenting software, VPN's, and a number of other categories. Custom application blocking gives us enhanced experiences on applications such as **YouTube, Vimeo, Twitter, Instagram**, and a number of other applications that offer safe enforced safe browsing options.

5. Additional Safeguards (From Business Broadband Providers) - Block Categories, Block Websites, Allow Websites

PROTECTING THE INDIVIDUAL

How the school builds resilience in its students to protect themselves and their peers through education and information

Guidance is detailed in the following documents/policies from the list at the beginning of this policy:

- Curriculum Policy
- PSHE Policy

Staff safeguarding professional development including on-line safety

Internet Safety, Social Media communication and cyberbullying are all constantly changing and developing areas impacting on the lives of our students and staff. The school keeps up to date with these issues through publications from the DfE, ISI, ISC, CEOP, ASCL, www.childnet.com, www.saferinternet.org.uk, CEOPEducation and other relevant organisations. Also, through discussing and listening to the students' own experiences and concerns about all these areas.

Staff are kept up to date on any issues & development relating to on-line safety through discussion at termly staff meetings and through communication in the weekly staff bulletin.

The Designated Safeguarding Lead is responsible for ensuring Filtering and Monitoring standards are met. The DSL should take lead responsibility for safeguarding and online safety.

Duties include overseeing:

- Filtering and monitoring reports
- Take the lead responsibility for any safeguarding concerns picked up by filtering or monitoring
- Encourage compliance of staff physically monitoring the screens of users and ensure that staff are aware of how to report concerns
- Weekly meetings with ICT staff for updates on filtering and monitoring systems and to assess whether the provision continues to meet the needs of the school
- Meetings with SLT and ICT staff to identify and ensure a thorough understanding of any current or potential risks
- Together with SLT and ICT staff review the Filtering and Monitoring provision annually. This should include the current provision, any gaps, teaching requirements and the specific needs of the students.

INCIDENT RESPONSE PROTOCOLS

Reporting mechanisms available for all users to report issues and concerns to the school and how they are managed and / or escalated

Incidents may require intervention by the IT department, such as removal of a programme or alterations to filtering systems.

The usual systems of reporting and following up concerns in the school apply:

- Students report concerns to their subject teacher, form tutor or directly to the Headteacher, Assistant Headteacher or any other member of staff they feel comfortable discussing or reporting a concern to.
- Staff keep the Headteacher informed of any issues or concerns that they have dealt with and the action they have taken. More serious concerns are passed on by staff and dealt with directly by the Headteacher, Assistant Headteachers, or other senior member of staff.
- Issues with Child Protection / Safeguarding implications would be referred to and dealt with by the Designated Safeguarding Lead as detailed in the Safeguarding Policy.
- If necessary, concerns would be escalated and reported to the appropriate authorities following DfE guidance as detailed in 'KCSIE'.

PARENT/CARER COMMUNICATION

Informing, communicating with and educating parents/carers in online safety

The parental newsletter is used to communicate with parents/carers about a wide range of issues which would include communication about online safety, social media and cyberbullying whenever relevant. This might be in response to issues in school or to issues in the national media, or it might include the dissemination of warnings or information that have been brought directly to the school's attention from external organisations.

Parents/carers can monitor communications and learning between the staff and their child through subject Google classrooms, our online learning platforms.

The school website has a secure area for parents/carers. Whenever the school is alerted to useful information / advice for parents/carers from reputable organisations, we put this advice in this section of the website and draw parents/carers' attention to it through our weekly newsletters.

Parents/carers and students are advised that the school is able to view, monitor and filter communications to or from student and staff email addresses

MANAGEMENT OF PERSONAL DATA

Please refer to our Data Protection Policy (see website).

All staff and volunteers sign our confidentiality statement as part of the recruitment procedure.

Parents/carers, students and staff are advised that the school is able to view, monitor and filter communications to or from student and staff email addresses