E-Safety Policy

The Olive Tree
Primary School

Document Control

This document has been approved for operation at The Olive Tree Primary School	
Date of approval:	14th November 2023
Date of next review:	November 2026
Review period:	As required / 3 years
Status:	Approved
Approval Committee:	SSIC
Version:	3.0

Contents **Page**

Scope of the Policy

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

We recognise that whilst working online it is essential that pupils are safeguarded from potentially harmful and inappropriate online material. As such, we have robust security in place such as appropriate filters and appropriate monitoring systems. These systems are regularly monitored, and staff are aware of these systems, they can manage them effectively and know how to escalate if a concern is identified.

The Education and Inspections Act 2006 empowers Heads of School/Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The Education Act 2011 increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published school Behaviour, Sanctions and Exclusion Policy.

The school will deal with such incidents within this policy and associated 'Behaviour, Sanctions & Exclusion', 'Safeguarding and Child Protection Policy' and 'Anti-Bullying' policies and will, where known, inform parents / carers of incidents of inappropriate online behaviour that take place out of school. Policies can be found on the school website.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the *school*:

Trustees:

- Trustees are responsible for the approval, review and effectiveness of the 'E-Safety' Policy. The Trustees receiving regular information about online incidents and monitoring reports will satisfy this requirement;

- All reports and monitoring information is shared with the Board of Trustees when and where applicable during termly Standards, Safeguarding and Inclusion Committee meetings.

Acting Head of School / Senior Leaders

- The Acting Head of School and senior leadership team has a duty of care to ensure the safety (including online) of members of the school community, though the day-to-day responsibility for ensuring online safety will be delegated to the Character Education and Behaviour Lead
- All staff should be aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff;
- The Acting Head of School / Senior leadership team are responsible for ensuring that the Character Education and Behaviour Lead and other relevant staff receive suitable training to enable them to carry out their roles and to train other colleagues, as relevant;
- The Acting Head of School / Senior leadership team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online monitoring role. This is to provide a safety net and also to provide support to those colleagues who take on important monitoring roles.

Designated Safeguarding Leads (DSL/DDSL) and the Character Education and Behaviour Lead

The DSL, Senior Leadership Team and staff are trained in online safety and are aware of the potential for serious child protection / safeguarding matters that arise from:

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

DSL / DDSLs & Character Education and Behaviour Lead will:

- take day to day responsibility for online safety and has a leading role

in establishing and reviewing the school 'E-Safety' Policy / documents;
- ensure that all staff are aware of the procedures that need to be followed in the event of an online incident taking place;
- provide training and advice for staff;
- liaise with the school ICT Support services partner;
- receive reports of online incidents and create a log of incidents to inform future online developments.

DSL will:

- meet regularly with nominated 'Safeguarding Trustee' to discuss current issues, review incident logs and filtering / change control logs;
- attend relevant meeting / committee of trustees;
- report regularly to the Senior Leadership Team.

Network Manager

The Network Manager will ensure:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- school meets required online technical requirements included those stipulated under the ESFA Risk Protection Arrangement (RPA);
- users only access the networks and devices through a properly enforced device management system;
- password protection policy, in which passwords are regularly changed;
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (Network Manager and DSL);
- Use of the network / internet / Showbie / Email / remote access is regularly monitored so misuse / attempted misuse can be reported to the Acting Head of School / DSL / Character Education and Behaviour Lead for investigation, action and/or sanction;
- the school web-filtering solution monitors all online activities.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- they have up to date online safety awareness and are familiar with the school's current 'E-Safety' Policy;

- they have read, understood and signed the staff 'Acceptable Use Policy' (AUP), where applicable;
- they report any suspected misuse or problem to the Acting Head of School / DSL / Character Education and Behaviour Lead for investigation, action and/or sanction;
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems;
- E-Safety principles are embedded in all aspects of the curriculum and other activities;
- pupils understand and follow the 'E-Safety' Policy and the 'conditions of use' under the Acceptable Use Policy (AUP);
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices;
- in lessons, where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found through internet searches.
- PREVENT guidance and understanding, refer to Safeguarding, Child Protection Policy, Educate Against Hate and Bolton-Safeguarding Against Harmful Radicalisation**.**

Pupils

Pupils are responsible for ensuring that:

- they are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy;
- they have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- they will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying;
- They will understand the importance of sharing of Nudes and Semi Nudes (also known as youth produced imagery)
- Sharing of nudes and semi nudes refers specifically to sharing nude and

semi-nude images and/or videos. We have a stand-alone policy on Sharing of Nudes and Semi Nudes that includes a flowchart. Staff will also refer to the Government guidance in relation to Sharing nudes and semi nudes: advice for education settings 2020. We also refer to 'Bolton Safeguarding Education Team's Safeguarding Practice Guidance: Responding to Nudes and Semi-Nudes Images and Videos,' available on the school website.

- We also promote the new Report Remove tool whereby children, young people and adults can report nude images of them that are circulating social media and ensure they are taken down.They understand the importance of adopting good online practice when using digital technologies out of school and realise that the school's 'E-Safety' Policy covers their actions out of school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, school website and information about national / local online safety campaigns / literature.

Parents and carers will be encouraged to support the school in promoting good online practice and to follow guidelines on the appropriate use of:

- school mobile devices at both school and home;
- digital and video images taken at school events;
- access to parents/carers sections of the website;
- their children's personal devices in the school (where this is allowed for medical purposes only).

Other Users

Other users who access school systems as part of the wider school provision will be expected to sign an AUP before being provided with access to school systems.

Teaching and Learning

Why Internet use is important

Digital literacy is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.

Digital literacy is also a part of the statutory curriculum and a necessary tool for staff and pupils to allow them to use computational thinking and creativity to understand and change the world.

Safer Internet Use

Access to the school's internet is designed with 'users' in mind, supported by a primary, and secondary 'firewall' and 'web-filtering' solution. We ensure that pupils are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum.

Pupils will be taught how to carry out safe and effective online research, to include the use of filters, and the implications of using copyright material to develop their digital literacy skills.

Evaluation of Internet Content

Pupils will be taught how to use internet derived materials to ensure both staff and pupils comply with copyright law.

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

The school's cyber security protocols (including the Firewall Solution, Primary and Secondary Web-Filtering Solutions, Global Proxy, and Mobile Device Management) will be reviewed regularly.

The Global Proxy system ensures that pupil devices are protected at home to the same level as when the devices are at school. Pupils have extended access to the internet whilst at school, whilst at home this is limited to whitelisted sites only. This supports parents/carers in managing their children's behaviour at home.

Email

Email accounts are administered and monitored by the school. Staff must immediately inform their line manager if they receive an offensive email. Email sent to an external organisation should be carefully written, ensuring email etiquette is adhered to in the same way as a letter written on school headed paper before sending. The forwarding of chain emails is strictly prohibited.

Published content and the school website

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The Acting Head of School will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work via school Website or X (formerly Twitter).

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Pupils' full names will not be used anywhere on the website or Twitter, particularly in association with photographs. Written consent will be sought from parents/carers prior to photographs of pupils being published on the school website.

Social Networking and Personal Publishing

The school will block/filter access to social networking sites. Pupils will be advised never to give out personal details of any kind which may identify them or their location. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. School staff will remain responsible for maintaining the school Twitter account allowing The Olive Tree Primary School to share pupil learning and experiences with parents, wider community and the world. This gives pupils access to experts, access to first hand research and gives them an audience to share learning with.

Filtering Solutions

The school will work with the Internet Service Provider (ISP) to ensure systems to protect pupils are reviewed and improved where necessary. If staff or pupils discover an unsuitable site, it must be reported to the ICT Support Services partner and the Acting Head School. The school ICT Support services partner will ensure that regular checks are made to ensure that the active filtering solutions remain fit for purpose. Weekly 'suspicious search' reports will be sent to the DSL and Acting Head of School for review. The school will follow necessary safeguarding protocols to ensure pupil safety, wellbeing and mental health (see appendix 1). See Appendix 2 for further information on the school's filtering and monitoring systems and its alignment with KCSIE2023.

Managing Video Conferencing

Only work related video conference calls should be made using school devices during the school day by staff.

Mobile Devices

Mobile phones must not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. Staff will use the school's telephone system to contact parents / carers. They will be given access to the school's mobile phone where the school's telephone system cannot be used (if staff are off-site).

Mobile devices (iPads) are used to support, enhance and transform teaching and learning in the classroom. Pupils are part of the 1:1 Family iPad programme which allows them to continue learning beyond school time (Flipped Learning).

Data Protection

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary

- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Personal data will be recorded, processed, transferred and made available in line with the school Pupil and Staff Privacy Notices.

Policy Decisions

Online Access Authorisation

- All staff, pupils and their parents/carers must read and sign an 'Acceptable Use Agreement' (AUP) before using any school IT resource.
- Online access is directly supervised by classroom staff across all year groups to ensure access to approved specific, online materials only.

Handling E-safety complaints

- The DSL and Acting Head of School will deal with any complaints in relation to internet misuse.
- Any complaint about internet misuse by staff must be immediately referred to the Acting Head of School.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents/carers will be informed of the complaints procedure.

Communications Policy

Introducing the E-Safety Policy to Pupils

- The school will continue to address matters in relation to 'E-Safety', and educate via termly assemblies, safer internet days and Relationship and Health Education (RHE) lessons. Educating our pupils on 'E-Safety' and staying safe online is a whole school responsibility, not just that of the Character Education and Behaviour Lead.
- Pupils will be informed that internet use to include online searches on the school network are monitored by the school and can be traced back to an individual user.

- Pupils will sign an 'AUP' setting out the rules for the use of mobile devices and the internet in and out of school.

Staff and the E-Safety Policy

- All staff will have access to the School 'E-Safety Policy' and its importance will be explained. 'E-Safety' and 'Prevent' training will be included as part of the induction process for any new starters.
- Staff should be aware that all internet use to include online searches on the school network are monitored by the school and can be traced back to an individual user. Discretion and professional conduct is essential.

Enlisting Parents/Carers Support

Parent/Carer attention will be drawn to the school 'E-Safety' policy in newsletters, the school prospectus and on the school Website.

School Support

Should the school have any concerns we will:

- Refer to the Department of Education guidance on Teaching online safety in schools **(**June 2019), Greater Manchester Procedures and UK Council for child internet safety (UKCCIS).
- Report to CEOP a law enforcement agency that keeps children and young people safe from sexual exploitation and abuse- Reporting link or Tel 0800 1111
- We access resources from the UK Safer Internet Centre to keep pupils safe online. We will also encourage our pupils/parents/carers to anonymously report online child sexual abuse imagery and videos to the UK Safer Internet Centre Hotline.
- Report any harmful content to - www.reportharmfulcontent.com

- Sharing nudes and semi nudes guidance - https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

- Safeguarding against harmful radicalisation - https://www.bolton.gov.uk/community-safety-anti-social-behaviour/safeguarding-radicalisation

- Educate against Hate - https://www.educateagainsthate.com/

- NSPCC ESafety for schools - https://learning.nspcc.org.uk/research-resources/schools/e-safety-for-schools

Appendix 1: Pupil iPad Suspicious Search Reports

Pupil iPad suspicious search report identifies blacklisted / unsafe searches (Via the 'Securly' student safety platform) See example of a Securly Suspicious Search report below

↓

DSL / DDSL notified of the search report with pupil details

↓

DSL / DDSL assesses the search and links it to the DDSL/Mental Health Lead

↓

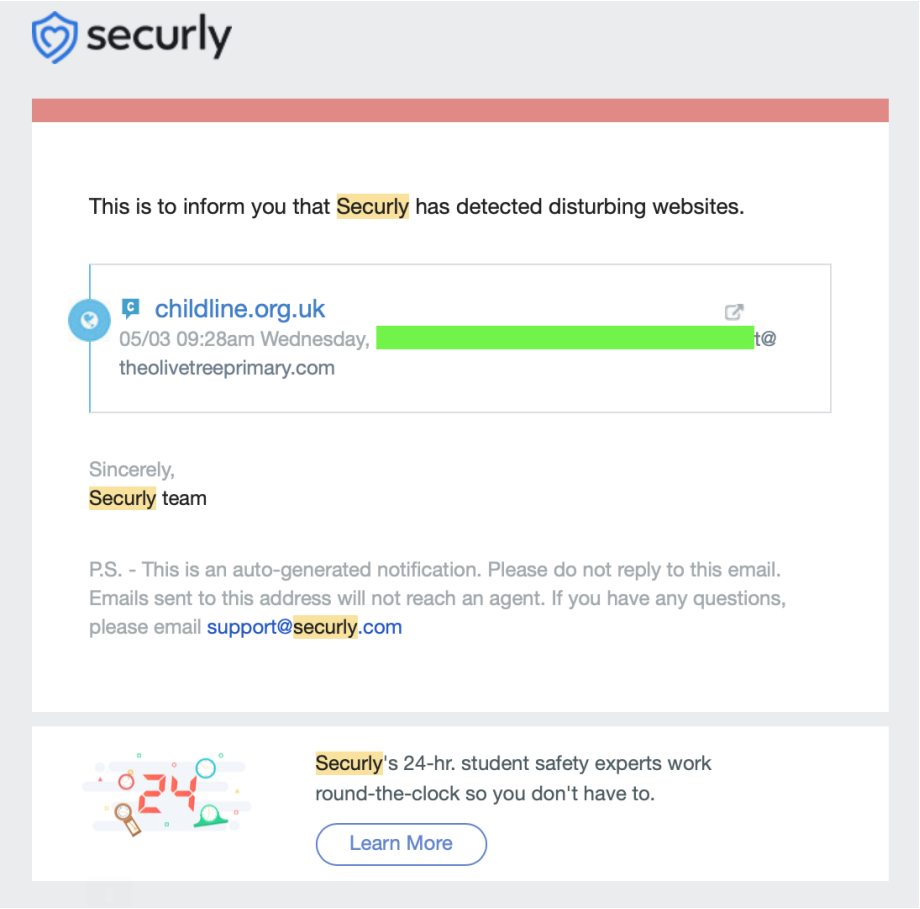
DSL/DDSL/Mental Health Lead to capture key information on CPOMS and link class teacher with next step actions

Based on the nature of the search, the following steps may take place instead of the steps above:

DSL to have a direct discussion with the child/parent/carer - update CPOMS logs

DSL to seek advice from the GMP Prevent Lead or LA Education Safeguarding Officer - update CPOMS logs

Example Securly Suspicious Search Report - (student name redacted in green)



General Actions:

1. **Low level** concern = Parent/carer informed, iPad cleared, general advisory discussion with parent/carer.
2. **Low to middle** concern = Parent/carer informed, iPad confiscated & cleared, meeting with parent/carer.
3. **Middle to high** level concern = Parent/carer informed, iPad confiscated, act on guidance given from GMP Police (Prevent Team) or The Education Safeguarding Officer.

Outside Agency contacts:

Prevent:
https://www.gmp.police.uk/advice/advice-and-information/t/prevent/prevent/
Tel: 0161 8566345
Lead: Wendy Robinson

Safeguarding
https://www.bolton.gov.uk/safeguarding-protecting-children/reporting-child-abuse/1
Tel: 01204 337472
Lead: Education Safeguarding Officer Jo Nicholson

Department for Education Guidance for schools on Policy for Prevent

The Prevent Duty: Departmental Advice for Schools and Childcare Providers June 2015 *This link doesn't work*
In order for schools and childcare providers to fulfil the Prevent duty, it is essential that staff are able to identify children who may be vulnerable to radicalisation, and know what to do when they are identified. Protecting children from the risk of radicalisation should be seen as part of schools' and childcare providers' wider safeguarding duties, and is similar in nature to protecting children from other harms (e.g. drugs, gangs, neglect, sexual exploitation), whether these come from within their family or are the product of outside influences.
Government Guidance on Online Safety in Schools. The school's curriculum (RHE, Science, Computing) supports teaching and learning on how certain actions, choices and decisions may impact one's own and the welfare of others.

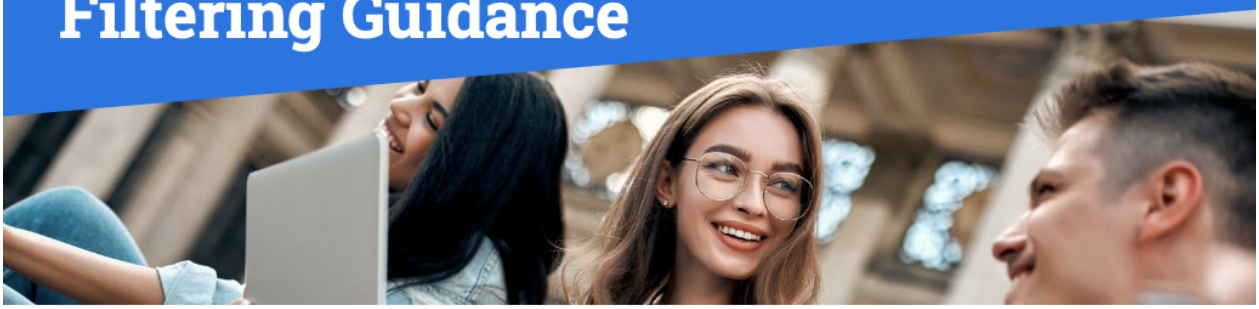
Teaching online safety in schools - GOV.UK

Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. We want schools to equip their pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world. This advice brings together information that will help schools deliver online safety content within their curriculum and embed this within their wider whole school approach. Refer to the education for a connected world framework for age-specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives. Through assemblies, RHE lesson, P4C lessons, Computing lessons, Educational visits and ESafety weeks; pupils learn how to use technology responsibly. They learn the rules of keeping safe online as well as how technology can be used positively. They learn how to be responsible and sign age appropriate use policies to support this. This is shared with parents/carers through information sessions, inductions, open days and newsletters. Parents and Carers sign agreements on how they can support children in using technology safely.

Appendix 2

How Securly Helps Schools Meet KCSIE Filtering Guidance

securly



Securly Filter is a web filter designed for schools and widely deployed in the UK and around the world. As UK government guidance evolves Securly makes every effort to ensure that its products comply and help schools comply with their statutory obligations around student safety and well-being.

filter

Securly Filter is one of a suite of school focused safety products from Securly designed to make it seamless for schools to meet their student safety obligations. Specifically, Securly Filter meets the filtering technical requirements, and Securly Aware and Securly Classroom help schools meet their KCSIE monitoring obligations.

Responses to KCSIE Web Filter Requirements

Make sure your filtering provider is:

KCSIE GUIDANCE	SECURLY RESPONSE
A member of Internet Watch Foundation (IWF).	Securly has been an IWF member since 01/03/2016.
Signed up to Counter-Terrorism Internet Referral Unit list (CTIRU).	Securly receives and incorporates the CTIRU feed into its filtering technology.
Blocking access to illegal content including child sexual abuse material (CSAM).	Securly blocks access to illegal content including CSAM.
If the filtering provision is procured with a broadband service, make sure it meets the needs of your school or college.	Securly works with broadband providers and managed service providers to ensure Securly Filter is well configured and fit for purpose.

Your filtering system should be operational, up to date and applied to all:

KCSIE GUIDANCE	SECURLY RESPONSE
Users, including guest accounts.	Securly Filter can be applied to all device types and all user categories in all locations, with user-level logging and filtering through sign-in and directory integration with Microsoft Azure or Google G-Suite. Securly's cloud architecture supports all device types (Windows, Chrome, iOS, MAC, Android, etc.) in all locations (in and away from school). It supports school-owned devices, guest networks, and BYOD.
School-owned devices.	Securly Filter can be applied to the school network, filtering all devices on the network and to individual school owned devices, of all types, including but not limited to windows, chrome, iOS, Android, Linux. School owned devices can then be filtered in any location.
Devices using the school broadband connection.	Securly Filter can also be applied to BYOD devices, and Guest networks ensuring all devices using the school broadband connection are appropriately filtered.

Your filtering system should:

KCSIE GUIDANCE	SECURLY RESPONSE
FIlter all internet feeds, including any backup connections.	Securly Filter can be applied at both the user/device level and at the network level.
Be age and ability appropriate for the users, and be suitable for educational settings.	Securly Filter is built exclusively for education and has school appropriate filtering configured out-of-the-box with simple configuration of more strict or relaxed policies as required. Through manual configuration or directory integration age appropriate (and other group) settings may be implemented.
Handle multilingual web content, images, common misspellings and abbreviations.	Securly Filter and it's classification engine PageScan (incorporation text scan and image scan) use dynamic categorisation, crowd sourced URL scanning, search engine crawling and paid 3rd party categorisation to keep its classification database up to date and to dynamically categorise new sites. This is an industry standard approach which covers text and images, is multilingual and handles common abbreviations and misspellings.
Identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them.	Securly works with schools to ensure Securly Filter is applied in the most robust way possible and includes publicly available best practice guides and recommendations for configuring devices and networks to best protect children and prevent circumvention.
Provide alerts when any web content has been blocked.	Securly Filter includes the ability to generate instant alerts for blocked content, this is configurable at a policy level to allow for different alert levels for vulnerable users.
Mobile and app content is often presented in a different way to web browser content. If your users access content in this way, you should get confirmation from your provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.	Securly Aware connects directly into Microsoft Office365 and G-Suite Workspace to scan documents, emails, chats, images, and videos for inappropriate content regardless of where those systems are used or how they are accessed.
It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the senior leadership team or the designated safeguarding lead.	Securly Filter categorises blocked URLs in a way designed to be useful in schools, Categories include pornography, drugs, gambling, hate and other adult. Students trying to access unsuitable material will be blocked, an alert is generated and the activity logged against the student. Appropriate staff may investigate via the reporting system.

Your filtering systems should allow you to identify:

KCSIE GUIDANCE	SECURLY RESPONSE
Device name or ID, IP address, and where possible, the individual.	Securly Filter logs the username from Microsoft Azure AD or G-Suite; for shared devices, a device name or serial number may be used instead, or where authentication is not possible, an IP address is recorded. This information determines if a device or user is on-site or off-site and if policies should differ based on that measure.
The time and date of attempted access.	The search term or content being blocked by Securly Filter and Securly Aware is logged and includes a date and timestamp for all activities.
The search term or content being blocked.	Securly Filter logs search terms in a format that is easy for non-technical users to inspect and understand.

KCSIE GUIDANCE	SECURLY RESPONSE
Physical Monitoring Physical monitoring can contribute where circumstances and the risk assessment suggests low risk, with staff directly supervising children on a one-to-one ratio whilst using technology.	**Classroom** Physical monitoring of devices on a 1:1 basis is time consuming and can be counterproductive to teaching and learning. Securly offers Classroom, a system that enables teachers to monitor all the devices in their class at once by displaying a thumbnail of each screen on a teacher's device and enabling teachers to zoom in on any particular student.
Internet and web access Some Internet Service Providers or filtering providers provide logfile information that details and attributes websites access and search term usage against individuals. Through regular monitoring, this information could enable schools to identify and intervene with issues concerning access or searches.	**Filter. Delegated Admin.** Securly Filter offers delegated administration enabling teachers and student safety staff to access filter logs and reports on students in their care. The interface is simple and non-technical. Reports can be customised, accessed at any time, or scheduled.
Monitoring Content Recognising that no monitoring can guarantee to be 100% effective, schools should be satisfied that their monitoring strategy or system (including keywords if using technical monitoring services) at least covers the following content.	**Aware** Aware helps schools monitor search, web browsing, and web based social media. And email, documents, drives, messaging, in Google and Microsoft environments. A sophisticated AI engine uses keywords and sentiment analysis to identify and categorise harmful activity. All categories identified in the technical guidance are covered.
Active monitoring where a system generates alerts for the school to act upon.	Aware generates real time alerts which are sent to the appropriate staff. Alerts may be tuned to minimise staff workload.
Pro-active monitoring where alerts are managed or supported by a specialist third-party provider and may offer support with intervention. Proactive monitoring is most effective where?	**On-Call** On-Call is a proactive monitoring service which utilises Securly's trained student safety team to analyse alerts and respond by logging cases and managing appropriate escalations.